U.S. Department of Justice

Federal Bureau of Investigation
Washington, D.C. 20535

June 8, 2016

MS. ALEXA O'BRIEN
MUCKROCK NEWS
DEPT MR 17650
POST OFFICE BOX 55819
BOSTON, MA 02205-5819

FOIPA Request No.: 1329073-000
Subject: Carnivore

Dear Ms. O'Brien:

Records responsive to your request were previously processed under the provisions of the Freedom of Information Act. Enclosed is one CD containing 605 pages of previously processed documents and a copy of the Explanation of Exemptions. Please be advised, these are the only copies of these documents located in our possession. The original copies of these documents could not be located for reprocessing.

Additional records potentially responsive to your subject exist. The Federal Bureau of Investigation (FBI) has located approximately 1,594 pages total of records potentially responsive to the subject of your request. By DOJ regulation, the FBI notifies requesters when anticipated fees exceed $25.00.

If all potentially responsive pages are released on CD, you will owe $40.00 in duplication fees (3 CDs at $15.00 each, less $5.00 credit for the first CD). Releases are made on CD unless otherwise requested. Each CD contains approximately 500 reviewed pages per release. The 500 page estimate is based on our business practice of processing complex cases in segments.

Should you request that the release be made in paper, you will owe $79.70 based on a duplication fee of five cents per page. See 28 CFR §16.10 and 16.49.

If you agree to receive all responsive material on CD, you will receive a $5.00 credit towards your first interim CD. As a result, we must notify you there will be a $25.00 charge when the second interim release is made in this case. At that time you will be billed for the $10.00 remaining from the $15.00 free of the first release, as well as the $15.00 duplication fee for the second release, for a total of $25.00.

Please remember this is only an estimate, and some of the information may be withheld in full pursuant to FOIA/Privacy Act Exemptions(s). Also, some information may not be responsive to your subject. Thus, the actual charges could be less.

Requester Response

No payment is required at this time. If your request does not qualify for eFOIA releases, you must notify us in writing within thirty (30) days from the date of this letter of your format decision (paper or CD). You must also indicate your preference in the handling of your request in reference to the estimated duplication fees from the following four (4) options:

☐ I am willing to pay estimated duplication/ international shipping fees up to the amount specified in this letter.

☐ I am willing to pay fees of a different amount.

Please specify amount: _____

☐ Provide me 100 pages or the cost equivalent ($5.00) free of charge. If applicable, I am willing to pay International shipping fees.

☐ Cancel my request.

If we do not receive your duplication format decision and/or estimated duplication fee selection within thirty (30) days of the date of this notification, your request will be closed. Include the FOIPA Request Number listed above in any communication regarding this matter.

For your information, Congress excluded three discrete categories of law enforcement and national security records from the requirements of the FOIA. See 5 U.S. C. § 552(c) (2006 & Supp. IV (2010). This response is limited to those records that are subject to the requirements of the FOIA. This is a standard notification that is given to all our requesters and should not be taken as an indication that excluded records do, or do not, exist.

You have the opportunity to reduce the scope of your request; this will accelerate the process and could potentially place your request in a quicker processing queue. This may also reduce search and duplication costs and allow for a more timely receipt of your information. The FBI uses a multi-queue processing system to fairly assign and process new requests. Simple request queue cases (50 pages or less) usually require the least time to process.

Please advise in writing if you would like to discuss reducing the scope of your request and your willingness to pay the estimated search and duplication costs indicated above. Provide a telephone number, if one is available, where you can be reached between 8:00 a.m. and 5:00 p.m., Eastern Standard Time. Mail your response to: **Work Process Unit; Record Information/Dissemination Section; Records Management Division; Federal Bureau of Investigation; 170 Marcel Drive; Winchester, VA 22602**. You may also fax your response to: 540-868-4997, Attention: Work Process Unit.

For questions regarding our determinations, visit the www.fbi.gov/foia website under “Contact Us.” The FOIPA Request number listed above has been assigned to your request. Please use this number in all correspondence concerning your request. Your patience is appreciated.

the Internet could have been paralyzed, disrupting several of the critical infrastructures that rely on the Internet for communication.

2. In testimony last February 16, you said that the FBI was producing "fast-developing leads" and that a break in the case was imminent. A couple of weeks later, Michael Vatis, director of NIPC, suggested that in fact agents were making slow progress in the case.

How would you assess progress in the case now?

In fact, the testimonies of FBI Director Freeh and NIPC Director Vatis were entirely consistent. Both cited the difficulties in conducting cyber crime investigations, but both also expressed optimism about the prospects for a successful resolution of the case. Director Freeh's February 16 testimony for the record contained the following remarks about the DDOS investigation:

> On February 8, 2000, the FBI received reports that Yahoo had experienced a denial of service attack. In a display of the close cooperative relationship the NIPC has developed with the private sector, in the days that followed, several other companies also reported denial of service outages. These companies cooperated with our National Infrastructure Protection and Computer Intrusion squads in the FBI field offices and provided critical logs and other information. *Still, the challenges to apprehending the suspects are substantial.* In many cases, the attackers used "spoofed" IP addresses, meaning that the address that appeared on the target's log was not the true address of the system that sent the messages.
>
> *The resources required in these investigations can be substantial.* Already we have five FBI field offices with cases opened: Los Angeles, San Francisco, Atlanta, Boston, and Seattle. Each of these offices has victim companies in its jurisdiction. In addition, so far seven field offices are supporting the five offices that have opened investigations. The NIPC is coordinating the nationwide investigative effort, performing technical analysis of logs from victims sites and Internet Service Providers, and providing all-source analytical assistance to field offices. Agents from these offices are following up literally hundreds of leads. While the crime may be high tech, investigating it involves a substantial amount of traditional police work as well as technical work. For example, in addition to following up leads, NIPC personnel need to review an overwhelming amount of log information received from the victims. Much of this analysis needs to be done manually. Analysts and agents conducting this analysis have been drawn off other case work. In the coming years we expect our case load to substantially increase. (Emphases added.)

NIPC Director Vatis' February 29 testimony for the record contained the following statement about the DDOS investigation:

On February 8, 2000, the NIPC received reports that Yahoo had experienced a denial of service attack. In a display of the close cooperative relationship that we have developed with the private sector, in the days that followed, several other companies (including Cable News Network, eBay, Amazon.com, Buy.com, and ZDNET), also reported denial of service outages to the NIPC or FBI field offices. These companies cooperated with us by providing critical logs and other information. *Still, the challenges to apprehending the suspects are substantial.* In many cases, the attackers used "spoofed" IP addresses, meaning that the address that appeared on the target's log was not the true address of the system that sent the messages. In addition, many victims do not keep complete network logs.

The resources required in an investigation of this type are substantial. Companies have been victimized or used as "hop sites" in numerous places across the country, meaning that we must deploy special agents nationwide to work leads. We currently have seven FBI field offices with cases opened and all the remaining offices are supporting the offices that have opened cases. Agents from these offices are following up literally hundreds of leads. The NIPC is coordinating the nationwide investigative effort, performing technical analysis of logs from victims sites and Internet Service Providers (ISPs), and providing all-source analytical assistance to field offices. Moreover, parts of the evidentiary trail have led overseas, requiring us to work with our foreign counterparts in several countries through our Legal Attaches (LEGATs) in U.S. embassies.

While the crime may be high tech, investigating it involves a substantial amount of traditional investigative work as well as highly technical work. Interviews of network operators and confidential sources can provide very useful information, which leads to still more interviews and leads to follow-up. And victim sites and ISPs provide an enormous amount of log information that needs to be processed and analyzed by human analysts.

Despite these challenges, I am optimistic that the hard work of our agents, analysts, and computer scientists; the excellent cooperation and collaboration we have with private industry and universities; and the teamwork we are engaged in with foreign partners will in the end prove successful. (Emphases added.)

Indeed, the FBI's investigation, conducted in close coordination with the Royal Canadian Mounted Police, very quickly had resulted in the identification of one subject in Canada. Because additional evidence needed to be gathered by the RCMP in the DDOS case and in another matter that came to light during the RCMP's investigation, the subject could not be immediately arrested, and the investigation's progress could not be discussed publicly. However, on April 15, the RCMP executed a search warrant and arrested a juvenile charging him with one of the attacks.

We would therefore assess the progress in this case as substantial and, indeed, unprecedented in a case of this scope and nature. The investigation continues into the attacks on DDOS victims, and we believe good progress continues to be made.

3. In testimony last February 16, you suggested that the FBI's resources "are stretched paper-thin" because of the lack of high-caliber government forensic computer experts.

How much has this contributed to the government's lack of success in catching the perpetrators of the February cyber attacks?

As discussed above, substantial progress in fact has been made in the DDOS investigation, with one subject already identified in Canada.

That said, given the explosive growth in computer crimes, our existing resources both in the Computer Analysis Response Team and in the NIPC and the related field office National Infrastructure Protection and Computer Intrusion Program are indeed stretched paper thin.

The Laboratory Division's CART team supports the investigation of any sort of criminal investigation in which evidence might be found on a computer (such as a drug trafficker's accounts) by conducting computer forensic examinations on seized media. The Lab's technically trained agents develop, deploy, and support equipment to perform Title III and FISA interceptions of data communications on the Internet. Staff in both of these areas (forensics and engineering support) is extremely stretched because these agents are tasked with providing support not only for cyber crimes, but all traditional crimes in which digital evidence may be present or data interception required.

The FBI's CART program, consisting of agents and analysts who examine digital medial in order to gather evidence, is not able to keep up with the increasing workload. The following is a summary of current and future trends assuming that the FBI Laboratory is funded for all pending budget requests:

CART Capacity and Backlog

Year	FTE Staffing	Capacity	Exam Requests	Case Backlog	Backlog Time (Months)
1999	95	1900	3500	1600	10.1
2000	104	2080	5000	2920	16.8
2001	154	3080	6000	2920	11.4
2002	213	4260	8500	4240	11.9

In addition, the FBI's Laboratory Division currently provides support not only for FBI cases, but also for the Drug Enforcement Administration and the Immigration and Naturalization Service.

The NIPC and the field office NIPCIP squads are responsible for conducting investigations of cyber attacks, including computer intrusions, viruses, and denials of service. The NIPC currently has 193 FBI Special Agents in the field offices investigating approximately 1200 computer intrusion and other "NIPCIP" cases. Only 16 Field Offices have full squads of seven or more agents. The other field offices have only 1 to 5 agents, who are responsible for not only cyber investigations, but also for industry liaison, the InfraGard Initiative, the Key Asset Initiative, and support to other investigative programs. Further, the NIPC lacks sufficient computer scientists and analysts to support the field office investigations. For instance, it has only 7 network analysts/electrical engineers to support investigations such as DDOS attacks.

The NIPC's and Field Office resources have remained relatively static. The NIPC Headquarters budget for fiscal years 99-01 has been as follows:

Fiscal Year	Budget Authority
1999	29,057,000 (included one-year funding of $10 million for special contingencies in Attorney General's Counter-terrorism Fund)
2000	19,855,000
2001 requested	20,396,000

Meanwhile, our pending case load has grown rapidly.

Fiscal Year	Pending Case Load at end of fiscal year
1998	601
1999	801
2000 (as of May 1)	1072

Clearly, then, resources have not kept pace with the crime problem.

Evidence gathering for computer intrusions mandates a prompt response because the digital evidence trail can disappear so quickly. The complexity of documenting, examining and analyzing the tremendous amount of information that is necessarily collected in these types of cases and its very technical nature requires investigators, examiners, and analysts with extremely

specific skills and experience. Because of the technical nature of this crime, it is difficult, if not impossible, to temporarily assign additional Special Agents to an investigation since a special technical skill set is required to investigate such matters.

Staff shortages impede not only our ability to conduct investigations adequately, but also to quickly obtain information, conduct analyses, and craft and issue appropriate warnings and alerts. This makes the Indications and Warning mission much more difficult to perform.

4. Some have argued that the high-profile February attacks on Yahoo, eBay, and other companies were just a diversion, allowing the hackers to focus on making smaller, intrusive attacks on smaller sites.

Have you found any evidence for this contention?

No. There are individuals and groups who do focus on planning and executing more intrusive attacks, often for the sake of stealing information or money, but we have not seen any correlation between such intrusions and the February DDOS attacks.

5. Why don't you think industry can solve this problem itself?

The Internet was not designed with security as the foremost consideration. Moreover, until very recently, security was not a major priority of either hardware/software manufacturers or consumers. As a result, networks are still rife with vulnerabilities. Improving security on the Internet is thus first and foremost the responsibility of industry. Government must protect its own systems, and can assist industry by providing information about threats and vulnerabilities that we are aware of, and the NIPC does that. But it is industry's responsibility to secure privately owned systems.

Even if systems were more secure, however, there would inevitably be some amount of computer crime committed on the Internet – including not just intrusions, denials of service, and viruses, but also traditional crimes perpetrated over the Internet such as fraud and dissemination of child pornography. As long as crime exists, the public will expect law enforcement to investigate and apprehend the perpetrators. And effective law enforcement is a key element in any strategy to deter further criminal activity. Thus, industry and law enforcement must work closely together.

6a. How big a problem is this for the FBI? Do you believe that there are important cyber attacks that are never investigated by law enforcement because the attacked companies refuse to report them?

The vulnerabilities that permeate the industry are a big problem for the FBI and other law enforcement agencies because they make it so easy for crimes to be committed. This accounts in

Senator Grassley

1. Of the 800 cases referred for criminal investigation in FY 1999 from the NIPC, what percentage of these cases were referred to other agencies, other than the FBI, for continued investigation and possible criminal prosecution?

As a general matter, the NIPC does not "refer" cases. Cases are normally initiated by a field office, whether a Field Office of the FBI, the Secret Service, another federal agency, or a state or local law enforcement agency. NIPC is the "program manager" of the FBI's computer intrusion investigative program, and so receives information about cases directly from the FBI Field Offices. Under PDD 63, other agencies are also supposed to report information about cyber incidents to the NIPC. Sometimes, NIPC will receive the first report of a cyber incident from a private company, a government agency, or another source, and contact the appropriate FBI Field Office. If another agency has concurrent investigative jurisdiction or some other non-investigative interest, that agency will also be contacted (either by the FBI Field Office of the NIPC). Where joint jurisdiction exists, the FBI field office may work jointly with the relevant other agencies (as discussed further below).

If an inquiry determines the complaint does not fall within the investigative guidelines of the FBI, it may be referred by the field office to another federal agency or to a state or local law enforcement agency which has the authority to conduct such investigations. FBI field offices develop liaison contacts with federal, state and local agencies investigating similar violations under federal or state statutes and complaints are disseminated through these liaison contacts. There is no system established to track how many complaints have been sent from FBI field offices to other law enforcement agencies.

There have been, however, several instances in which the NIPC or an FBI field office has contacted another agency to determine if that agency wanted to conduct an investigation either jointly or separately, but that agency declined. A couple of examples are listed below.

In May 2000, the FBI's Detroit Field Office referred a complaint to the local Secret Service office regarding a denial of service attack against NHL.com, going so far as to transfer the call from the FBI field office to the Secret Service field office. The Secret Service told the complainant that no one was in the office to receive the complaint due to a visit of Texas Governor George W. Bush to Michigan. The complainant then called the FBI again and the Detroit Field Office took the complaint and assigned the matter for investigation.

Also in May 2000, based on FBI source information, the NIPC notified the USSS headquarters that there may be a vulnerability with the White House Webpage that gave the public access to all the files on that server. The USSS advised that the system administrator may already be aware of this. Neither the NIPC nor the FBI's Washington Field Office has heard back from the USSS regarding this matter.

In another instance, the FBI's Williamsport, Resident Agency, part of the Philadelphia Field Office, opened an investigation into a series of computer intrusion into 10 companies resulting in the loss of approximately 28,000 credit card numbers. During the initial investigation, the FBI discovered that one of the victims located in Buffalo, NY, had contacted the Secret Service and the USSS had opened a case pertaining to the intrusion against the single victim company, but was not investigating the larger set of thefts. The FBI contacted the Secret Service Division in Buffalo, NY to coordinate the case, since USSS already had a pending investigation. The FBI was told that due to the Security Detail Duties for the First Lady, the USSS would be unable to coordinate at the present time with the FBI on the case.

In addition, the FBI has worked, and continues to work, many investigations jointly with other agencies. Two notable examples include Solar Sunrise and Moonlight Maze. Both cases involved extensive intrusions into Department of Defense and other government agency computer networks. The investigations involved an NIPC-coordinated investigation involving numerous law enforcement, intelligence, and defense agencies, as well as foreign law enforcement agencies.

Beyond those examples, the following are other instances of joint investigations.

DDOS: Numerous Internet commerce sites have been victimized by DDOS attacks since February 7, 2000. These DDOS attacks prevented the victims from offering their web services on the Internet to legitimate users. A DDOS attack uses compromised computer networks to "flood" a victim's computer network with massive amounts of data, which causes the victim's computer network to become overwhelmed and to stop operating. The DDOS attack investigation are investigations in seven FBI field offices, five overseas Legal Attache offices, other government agencies such as NASA, as well as the Royal Canadian Mounted Police. Reflecting the extraordinary level of cooperation on these investigations, on April 15, 2000, the Canadian officials arrested a juvenile charging him with one of the attacks.

Curador: On March 1, 2000, a computer hacker using the name, "Curador", allegedly compromised multiple E-commerce websites in the U.S., Canada, Thailand, Japan and the United Kingdom, and apparently stole as many as 28,000 credit card numbers. Thousands of credit card numbers and expiration dates were posted to various Internet websites. On March 9, 2000, InternetNews reported that Curador stated, "Law enforcement couldn't hack their way out of a wet paper bag. They're people who get paid to do nothing. They never actually catch anybody." After an extensive international investigation, on March 23, 2000, the FBI assisted the Dyfed Powys (UK) Police Service in a search at the residence of Curador; Curador, age 18, was arrested in the UK, along with an apparent co-conspirator under the Computer Misuse Act 1990. Under United Kingdom law, both males have been dealt with as adults. Loss estimates are still being determined.

This case was predicated on the investigative work by the Dyfed Powys Police Service, the Federal Bureau of Investigation, Internet security consultants, the Royal Canadian Mounted Police, and the international banking and credit card industry. This case illustrates the benefits of

law enforcement and private industry, around the world, working together in partnership on computer crime investigations.

Burns: In August 1998, the FBI initiated an investigation on an individual only known as "zyklon," who conducted numerous computer intrusions to various computer systems causing damages to websites and system files. The case was worked in cooperation with the Virginia State Police. The investigation identified zyklon to be Eric Burns of Shoreline, Washington. In February 1999, following an execution of a search warrant, Burns confessed to the intrusions. In May 1999, Burns also gained unauthorized access and defaced the webpage for the White House website. At that point the FBI began working with the U.S. Secret Service on the case. In September 1999, Burns pleaded guilty to one count for violation of Title 18 USC Section 1030 (Computer Fraud and Abuse) for one of the 1998 intrusions. In the plea agreement, Burns also admitted his criminal activity into several other intrusions including the White House website. In November 1999, Burns was sentenced to 15 months in prison, 3 years supervised release and $36,240 in restitution and a $100 fine.

Trifero: This investigation was worked jointly with the Middletown Rhode Island Police Department, the state Office of the Inspector General (OIG), National Aeronautics and Space Administration (NASA), and the FBI. Sean Trifero compromised various company and University computer systems, including systems maintained by Harvard University, Amherst College, Internet Services of Central Florida, Aliant Technologies, Arctic Slope Regional Corporation and Barrows Cable Company. He would utilize these compromised systems to establish web pages, E-Mail and Internet Relay Chat (IRC) Groups in the background of the victim's computer system. Trifero would also provide others with access to these compromised systems. On 10/6/1998, Trifero entered a guilty plea in the District of Rhode Island, in connection with this matter. On 2/22/1999, Trifero was sentenced in connection with his guilty plea to five counts of violating Title18 United States Code, Section 1030. He was sentenced to: 12 months plus 1 day in jail; $32,650.54 in restitution; $500 special assessment; three years supervised release; five hours/wk community service for 36 months; use of the Internet, but no contact with members of any hacking/cracking group.

Mewhiney: Throughout 1996, National Oceanic and Atmospheric Administration (NOAA) suffered several computer intrusions which were also linked to intrusions occurring a the National Aeronautics and Space Administration (NASA). These computer intrusions continued through 1997. The FBI worked the case jointly with NOAA, NASA, and the Canadian authorities and identified the subject, Jason G. Mewhiney, who resided in Canada. The original damage assessment that Mewhiney had caused, exceeded $40,000. In April 1999, Jason G. Mewhiney was indicted by Canadian authorities. In January 2000, Mewhiney pleaded guilty to 12 counts of intrusions which included violations spanning from May 1996 through April 1997, of destroyed/altered data and intrusions with the intent to damage. In the Canadian Superior Court of Justice, Mewhiney was sentenced to 6 months in jail for each of the counts to run concurrently.

Bliss: In February, 1998, the FBI opened an investigation to assist the U.S. Air Force and U.S. Navy regarding multiple computer intrusions. The case was worked jointly with the U.S. Naval Criminal Investigative Service and Florida State Attorney's Office in Jacksonville, FL. The subject was identified as Jesse Le Bliss, a student of the University of North Florida. On August 21, 1998, Bliss pleaded guilty to one felony count for violation of Florida State Statute 815.06 entitled, Offenses Against Computer Users. On September 19, 1998, Bliss was sentenced in the Fourth Judicial Circuit, State of Florida, to six months house arrest followed by three years probation, 200 hours of community service, and a written letter of apology to the Commandant of the United States Marine Corps.

CD Universe: One pending case being worked by the FBI's New Haven Division and the U.S. Secret Service has been widely reported in the press, due to statements made to reporters by the alleged perpetrator. In December 1999, the FBI's New Haven Division opened a case into intrusions into the computers of CD Universe, an on-line music seller, and the theft of customers' credit card numbers and a related extortion threat. Because of the credit card aspect, the FBI called the USSS to ask if USSS wanted to investigate jointly. The USSS declined. In January 2000, the New York Times ran a front page story about the case, based on conversations between the reporter and the alleged perpetrator. Subsequently, USSS called the FBI back and requested to work the case jointly. That case is still pending.

Other

There are other investigations that are being conducted with other agencies, however further details may adversely impact the investigation due to their pending status. There are currently 47 pending investigative cases which are being worked jointly between the FBI and the multiple entities of the Department of Defense. An additional 58 cases were investigated jointly with other entities that are now in closed status.

2. If some of the referred cases are potential violations that are traditionally enforced and investigated by other agencies, please describe your mechanisms and procedures that allow for cyber investigations to be conducted by those particular law enforcement agencies (other than the FBI).

The primary statute used by the FBI in computer intrusion investigations is Title 18, USC, 1030. Under this statute, the FBI has broad authority to investigate computer crime offenses. In instances where the computer crime does not meet FBI jurisdiction, the local FBI field office will refer the complainant to the appropriate law enforcement agency (federal, state, or local) which has authority to conduct the investigation. On other occasions, the FBI may continue to work a matter jointly with another law enforcement agency, even if they do not have primary jurisdiction, to provide needed resources and technical expertise. FBI field offices develop liaison contacts with state and local agencies investigating similar violations under state statutes and complaints are disseminated through these liaison contacts. The above cited credit card case is an example of

how the FBI field offices make direct contact with their counterpart field offices, such as US Secret Service, to coordinate aspects of an investigation.

3. Please specifically cite the number of NIPC referred cases that have a direct impact or posed a threat on the nation's critical infrastructures.

The nation's "critical infrastructures" are those physical and cyber-based systems essential to the minimum operations of the economy and government, including telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private. One of the most difficult aspects of cyber investigations is that it is not clear at the outset what the extent of the threat, or the potential damage to networks, is. Each case must be thoroughly investigated to determine the level of threat and compromise. What seems like a relatively minor incident might turn out to be very significant, and vice versa. This means that it is much more difficult for field investigators to use traditional investigative thresholds in determining how to utilize scarce resources. Moreover, computer systems and networks employ trusted relationships between other computer system and networks, based upon the users' privileges. If a computer system or network is root-level (or super user) access compromised, the threat potential is substantial, and could theoretically pose a major threat to other trusted systems. This means that "critical infrastructure" systems are often connected with, and affected by, systems that are in and of themselves not critical.

The existing NIPC database does not classify cases by critical infrastructure at this time. Thus, there is no methodology to determine which cases ultimately involve a threat to our nation's critical infrastructure.

The Distributed Denial of Service (DDOS) attacks launched in February of this year are a good example of the difficulty of categorizing an attack as an "infrastructure" attack or some lesser sort of attack. In a Distributed Denial of Services attack, not only are the "victim" systems affected, but also the thousands of computer systems and networks that were, unknowingly, infiltrated and used to carry out the attack, and Internet Service Providers that were heavily trafficked during the attack. All of the computer systems and networks that participated in the attack were compromised. Moreover, even though the effect of the attacks was relatively ephemeral and brief, the knowledge gained by analyses of these attacks is critical to our ability to protect against more devastating attacks in the future. If the DDOS attacks had been directed against the major Internet hubs rather than against primarily e-commerce companies, traffic on the Internet could have been paralyzed, disrupting several of the critical infrastructures that rely on the Internet for communication.

4. Please describe the job description and agency of any state and local law enforcement officials currently assigned to NIPC on a full time basis at FBI Headquarters.

The FBI currently has one local law enforcement officer assigned to the NIPC. He is from the Tuscaloosa County Sheriffs Department and his principal job is to work on outreach initiatives

to state and local law enforcement as part of the FBI's responsibility as the "Lead Agency" to work with the "Emergency Law Enforcement Services Sector" under PDD-63. He has also participated in the delivery of training to field investigators under our Key Asset Initiative. This representative replaced an earlier representative from the Oregon State Police, who rotated back to his home agency. The NIPC is also in discussions with several Washington, D.C. area police departments about having officers detailed to the NIPC on a full- or part-time basis.

5. Please describe any private sector representatives, past or present, who voluntarily participate in the Center to facilitate sharing of information between NIPC and the private infrastructure owners and operators.

The NIPC works on a daily basis with private sector representatives to share information. This occurs through such initiatives as InfraGard, which provides information to infrastructure owners and operators on a daily basis, and the pilot project for Indications and Warning that the NIPC has established with the electrical power sector under the auspices of NERC, and the Key Asset Initiative. It also occurs on a case by case basis as we disseminate targeted or general alerts or warnings to industry. The NIPC also works closely with private sector contractors who assist with technical analysis and information sharing.

In addition, the NIPC is working with the Information Technology Association of America to bring private sector representatives into the Center for a period of time as "detailees." That is part of a cybercrime initiative sponsored by the ITAA and the Attorney General.

6. Please describe any private sector representatives that are hired and paid by NIPC funds.

The NIPC has hired contractors to support our work in analyzing cyber intrusions into the infrastructures as well as to provide technical support to our investigations. In addition, a representative from Sandia National Laboratories, has been working at the Center. The NIPC has been reimbursing the Department of Energy under the Interagency Personnel Act for the cost of this detailee's contract.

7. On page 16 of your written testimony, you state: "the FBI, on behalf of the law enforcement community should enhance its technical capabilities (encrypted evidence)." Shouldn't all law enforcement agencies, from federal to state require this capability to accomplish the NIPC mission ?

As noted on page 16 of the written testimony, the law enforcement community is extremely concerned about the serious public safety threat posed by the proliferation and use of strong, commercially-available encryption products that do not allow for law enforcement access to the plaintext of encrypted, criminally-related evidence obtained through court-authorized electronic surveillance and/or search and seizure. The potential use of such non-recoverable encryption products by a vast array of criminals and terrorists to conceal their criminally-related communications and/or electronically stored information poses an extremely serious threat to

public safety and national security.

In order to address this serious threat and as noted in the written testimony, it is imperative that law enforcement enhance it technical capabilities in the area of plaintext access to encrypted evidence. As part of the government's approach to the encryption issue, the Administration has expressed support for and has proposed the creation of a law enforcement Technical Support Center within the FBI for the purpose of providing the entire law enforcement community with urgently needed plaintext access technical capabilities necessary to fulfill its investigative responsibilities in light of the proliferation of strong, commercially-available encryption products within the U.S. In fact, included in the Administration's Cyberspace Electronic Security Act of 1999 which was forwarded to the Congress last September is a provision that authorizes to be appropriated $80 million to the FBI for the creation of the Technical Support Center, which will serve as a centralized technical resource for federal, state and local law enforcement in responding to the ever increasing use of encryption by subjects of criminal cases.

The TSC is envisioned as an expansion of the FBI's Engineering Research Facility (ERF) to take advantage of ERF's existing institutional and technical expertise in this area. This approach represents a cost effective, non-duplicative and efficient means of provide every U.S. law enforcement agency with access to technical capabilities needed to address lawfully seized encrypted evidence and is supported by the International Association of Chiefs of Police, the National Sheriff's Association and the National District Attorney Association as well as the Information technology industry.

8. Please describe which agencies were in the past participating in the NIPC, but are no longer members. Describe the reasons given by those agencies to the FBI for their withdrawal from participation.

One of the difficulties in attempting to operate an interagency Center is ensuring that all relevant agencies participate. Agencies have not received direct funding to participate in the Center, and so must take detailees to the NIPC out of existing personnel resources. In addition, personnel with cyber expertise are unfortunately in very short supply, meaning that agencies must commit to take scarce resources and send them outside their agencies. Despite these impediments, numerous agencies have sent detailees to the NIPC, including: Defense/Office of the Secretary of Defense; Central Intelligence Agency; National Security Agency; Air Force Office of Special Investigations; U.S. Navy; U.S. Army; U.S. Postal Service; Defense Criminal Investigative Service; General Services Administration; U.S. Air Intelligence Agency; Department of Commerce, and the Tuscaloosa, AL Sheriff's office. In addition, we have foreign liaison representatives from two allied countries who assist in coordinating international activities with our counterparts. A representative from FAA is also scheduled to start at the end of June. Additional representative from DoD, CIA, and NSA are also slated to arrive in the near future. We are also expecting representatives from local Washington area police departments on a part-time basis.

Some agencies were represented earlier but do not currently have representatives. Circumstances necessitated the recall of the first State Department representative. State agreed to do so, and has committed to NIPC that it would replace him with two new representatives. DoE's first representative rotated back after more than two years. NIPC's understanding as to why this representative rotated back is that he was at NIPC for a lengthy time and was needed at DoE headquarters to assist in a DOE reorganization. DoE has committed to replacing that detailee.

Secret Service earlier had two detailees to the NIPC, but recalled those detailees and has not yet committed to replacing them. Secret Service has not provided any written explanation for this, but in oral discussions, Secret Service officials stated that USSS was not getting additional funding for its electronic crimes program despite its participation in NIPC; the FBI was receiving more media attention in the cyber crime area; and NIPC had not "referred" cases to Secret Service for investigation. NIPC offered any support it could give to Secret Service in addressing budget requests; noted that NIPC public statements often referred to partnership with USSS; and offered to do more to support USSS initiatives with public statements and case analyses. NIPC also stated (as discussed further below) that its role is not to create and "refer" cases; rather, cases generally originate in Field Offices, and FBI and Secret Service field offices frequently work computer crime cases together.

NIPC fully recognizes the value other agencies bring to the cyber crime and infrastructure protection mission. That is why NIPC is an interagency Center, and has senior managers from other agencies in addition to investigators and analysts. For instance, the NIPC Deputy Director is from DoD/OSD; the Section Chief of the Analysis and Warning Section is from CIA; the Assistant Section Chief of the Computer Investigations and Operations Section is from Air Force OSI; the Unit Chief of the Analysis and Information Sharing Unit is from NSA; and the Unit Chief of the Watch and Warning Unit is from the U.S. Navy. Secret Service formally occupied the position of Assistant Section Chief of the Training, Outreach, and Strategy Section. Recognition of the need for other agency participation is also what drives NIPC to continually seek additional representatives from other agencies. It is also reflected in the numerous joint investigations that NIPC and FBI Field Offices have been involved in with other agencies (as discussed further below).

Senator Leahy:

1. Can an attempt to commit a violation of 18 U.S.C. § 1030 (a)(5) currently be prosecuted under the attempt provision found in 18 U.S. C. § 1030(b), even if the attempt does not result in loss of at least $5,000 or cause one of the other results listed in § 1030 (e)(8)?

The question calls for an answer interpreting prosecution authority under statute, and as such, is more appropriately propounded to the Department of Justice. As a general rule, however, the FBI understands that, under certain factual circumstances, 18 U.S.C. § 1030(b) does allow for the prosecution of violations of 18 U.S.C. § 1030(a)(5) even if the attempt does not result in a loss of at least $5,000 where evidence demonstrates the offender's specific intent was to cause a loss

in excess of $5,000.

2. If an attempt cannot be so prosecuted, would amending the statute so that the aggravating factors included in the definition of "damage" in 18 U.S.C. §§ 1030 (e)(8)(A)-(D) are instead moved to be elements of the offense under § 1030 (a)(5) change that result?

The question calls for a hypothetical interpretation of a statutory amendment as applied through the substantive case law of "attempt," and should be directed to the Department of Justice for a more detailed and definitive response. As a general matter, however, the FBI does not understand that elevating the definitional elements of the term "damage" to become substantive elements of section 1030 offenses will, in all circumstances, resolve the attempted offense issues generated by the facts of most investigations. Instead, the FBI favors an approach which would combine a restructuring of the elements of the definition of "damage" into the penalty provisions of section 1030(c) with the creation of a lesser offense for those circumstances where damages of $5,000 or more cannot be substantiated. The FBI believes that some unauthorized access intrusions into computers affecting interstate commerce (i.e., protected computers) are so inherently violative as to justify Federal criminal sanctions even where there is no change affecting the integrity or availability of data or where the actual damages suffered do not attain the $5,000 threshold. The intentional unauthorized computer intrusion into the privileged and private medical records of citizens is but one such example. Such a statutory approach as has been suggested by DoJ's Computer Crime and Intellectual Property Section (CCIPS) would create a lesser included misdemeanor offense where the $5,000 threshold is not, in fact, demonstrated and would provide jurors in cases involving damages close to the threshold a legitimate alternative for otherwise violative behavior.

3. If a definition of "loss" were added to § 1030(e) to define loss as "the reasonable cost to any victim of responding to the offense, conducting a damage assessment, restoring data, programs, systems or information to their condition prior to the offense and any revenue lost or costs incurred by the victim as a result of interruption of service," would the $5,000 threshold be easier to meet than under current law?

The FBI favors any amendments which allow for the increased inclusion of any costs, losses or other expenditures that a victim would not have reasonably incurred but for the violation regardless of whether those losses resulted from an actual interruption of service. The FBI favors such a definition which would also include, if reasonable, the cost of system reconfiguration related to deterring or eliminating similar future violations.

4. With respect to violations of § 1030(a)(5)(A), is it your understanding that each separate "transmission" could form the basis of a separate count? Similarly, with respect to violations of §§ 1030(a)(5)(B)-(C), is it your understanding that each separate "intentional access[ ] " could form the basis of a separate count?

The question calls for an interpretation of a statute applying the substantive case law of

what constitutes "criminal episode," and related concepts of what constitutes appropriate "joinder," or "severance" under the Federal Rules of Criminal Procedure and should more appropriately be directed to the Department of Justice for a detailed and definitive response. As a general matter, however, the FBI understands that whether a single computer transmission of malicious code under section 1030(a)(5) may form the basis for a single count under an indictment will, in large measure, turn upon the unique facts of any given investigation. Whether a single transmission of a self-replicating, self transmitting destructive computer virus constitutes one transmission, and therefore one count, or thousands of transmissions intentionally effectuated by chain reaction, and therefore thousands of counts, may turn upon an evaluation of numerous factors not the least of which would include the object and intent of the offender/transmitter, the design of the code, the reasonable foreseeability of re-transmission and, as a practical matter, the ability to track, gauge and prove the re-transmission. Similarly, whether, in a computer network environment, the repeated unauthorized accessing of a computer in violation of section 1030(a)(5)(B)-(C), which accessing is temporally related, will, as a practical matter, frequently turn upon the configuration of the network and its security and banner system, to name but a few factors.

5. Are you aware of any cases in which the current statutory maximum terms of imprisonment under 18 U.S.C. § 1030 were insufficient to effect the sentence called for by the Sentencing Guidelines, including using the provisions of U.S.S.G. § 5G1.2, which provide that sentences on multiple counts may be imposed consecutively to the extent necessary to produce a combined sentence equal to the total punishment called for by the guidelines?

The NIPC referred this question to the Department of Justice Computer Crimes and Intellectual Property Section for input. The Department reported that it could recall no cases in which the current statutory maximum terms of imprisonment under 18 U.S.C. § 1030 were insufficient to effect the sentence called for by the Sentencing Guidelines, including using the provisions of U.S.S.G. § 5G1.2.

6. Please explain the reason, if any, to continue the codification of the work-sharing agreement between the Secret Service and the Federal Bureau of Investigation found in § 1030(d)?

In 1996, Congress specifically limited the Secret Service's authority to investigate crimes under 18 U.S.C. § 1030 to those offenses under subsections (a)(2)(A) and (B), (a)(3), (a)(4), (a)(5) and (a)(6). The Senate Report accompanying the 1996 amendment explained that:

> [t]he new crimes proposed in the bill, however, do not fall under the Secret Service's traditional jurisdiction. Specifically, proposed subsection 1030(a)(2)(C) addresses gaps in 18 U.S.C. 2314 (interstate transportation of stolen property), and proposed section 1030(a)(7) addresses gaps in 18 U.S.C. 1951 (the Hobbs Act) and 875 (interstate threats). These statutes are within the jurisdiction of the Federal

Bureau of Investigation, which should retain exclusive jurisdiction over these types of offenses, even when they are committed by computer.

S. Rep. No. 357, 104th Cong., 2d Sess. 13 (1996).

Inherent in the 1996 changes was the recognition that the statute was being amended to reflect the respective investigative jurisdictional limits existing at that time. It was clear at that time that the jurisdiction of the Secret Service, found at 18 U.S.C. § 3056, did not encompass the types of offenses described in Section 1030 (a)(1), (a)(2)(C), or (a)(7).[1] Given that there have been no additional grants of general investigative jurisdiction to the USSS since that amendment, it is not clear why the USSS's jurisdiction over computer crimes under Section 1030 should be expanded. The theft of National Security information which is the type of information Section 1030(a)(1) was intended to address has never been the subject of USSS jurisdiction. In addition, the types of crimes contemplated by 1030(a)(2)(C) and (a)(7), as recognized by the legislative history, have traditionally been investigations solely in the province and expertise of the FBI.

The 1996 provision is an explicit effort by Congress to address the criminal offenses at issue through a division of labor primarily determined by investigative responsibility and expertise. Any reversion to the pre-1996 jurisdictional provisions raises serious issues and concerns about the utilization of resources and proper coordination. Concurrent jurisdiction would result in a duplication of efforts that would waste resources and encourage independent investigations by separate agencies at the expense of coordinated joint efforts. Indeed, given the decision by Secret Service to refrain from participation in the National Infrastructure Protection Center (NIPC) (both by detailing personnel and providing investigative information from its cases) despite a mandate from the President to do so under PDD-63, expanding USSS's cyber jurisdiction at this time would result in a fractured approach to sensitive intrusion investigations involving espionage, extortion, and other serious matters.

7. The FBI has limited authority to issue administrative subpoenas in certain cases, such as federal health care fraud or sexual exploitation or other abuse of children. Since cybercrime cases are criminal in nature, is the FBI able to obtain documents relevant to the investigation with grand jury subpoena? To the extent that documents obtained with a

---

[1] "Under the direction of the Secretary of the Treasury, the Secret Service is authorized to detect and arrest any person who violates --

(1) section 508, 509, 510, 871, or 879 of this title or, with respect to the Federal Deposit Insurance Corporation, Federal land banks, and Federal land bank associations, section 213, 216, 433, 493, 657, 709, 1006, 1007, 1011, 1013, 1014, 1907, or 1909 of this title;

(2) any of the laws of the United States relating to coins, obligations, and securities of the United States and of foreign governments; or

(3) any of the laws of the United States relating to electronic fund transfer frauds, credit and debit card frauds, and false identification documents or devices; except that the authority conferred by this paragraph shall be exercised subject tot he agreement of the Attorney General and the Secretary of the Treasury and shall not affect the authority of any other Federal law enforcement agency with respect to those laws.

grand jury subpoena need to be shared with third-party experts, can permission be obtained to do so under Federal Rule of Criminal Procedure 6(e)(3)?

Generally speaking, a "governmental entity" is authorized under 18 U.S.C. 2703 (b) (1) (B) to obtain the contents of an electronic communication in *remote computer storage* with prior notice, as delimited in 18 U.S.C. 2703(b) (2), by using an administrative or grand jury subpoena. A governmental entity is also authorized under 18 U.S.C. 2703(c)(1)(C) to obtain certain subscriber or customer information from a provider of electronic communication services or remote computing service, by using an administrative, grand jury, or trial subpoena, or as otherwise permitted under 18 U.S.C. 2703 (c)(1)(B). The Electronic Communications Privacy Act (ECPA) does not itself identify which federal agencies qualify as "government entities" authorized to issue administrative subpoenas. Currently, the FBI is authorized to issue administrative subpoenas in cases involving health care fraud under 18 U.S.C. §3486 and in cases involving child pornography and sexual solicitation under 18 U.S.C. §3486A. Unfortunately, there does not currently exist a statute authorizing or designating the FBI as a "governmental entity" authorized to issue administrative subpoenas for violations of 18 U.S.C. § 1030 or other crimes of fraud increasingly committed by or facilitated through the use of a computer. The absence of such a statute impedes FBI efforts to accelerate an effective response to cyber crime.

While helpful, the use of grand jury subpoena to acquire minimally intrusive transactional information (e.g., so-called "header information" such as "to" or "from") or subscriber information (e.g., the name and address of the owner of an Internet screen name) is frequently a cumbersome and time consuming process especially in investigations where time is of the essence or where the information sought is from an unusually large number of providers. Some circumstances may dictate seeking express court authorization under the provisions of Federal Rule of Criminal Procedure 6(e)(3)(C) for disclosure to non-government experts who may not qualify as personnel assisting the attorney for the government in the investigation before the grand jury. In many cases, the practical concerns of delay and coordination with other agencies and courts further stymies government's ability to provide a timely response to imminent criminal behavior.

The FBI supports an expansion of its statutory authority to issue administrative subpoena under the Electronic Communications Privacy Act for any violation of law within the FBI's existing criminal investigative jurisdiction. The FBI's experience to date in the issuance of administrative subpoena in the areas of health care fraud and child exploitation crimes demonstrates that it can responsibly limit and control the exercise of this authority.

8. Denial of service attacks are increasing exponentially. According to the FBI, these attacks involve the placement of tools such [as] Trinoo, Tribal Flood net, TFN2K or Stechenldraht on unwitting victim systems, which then send messages upon remote command to a targeted computer system until that system is overwhelmed and essentially shut[s] down. In order to document in real-time the remote command being given and the triggering of the message flood to the target system, is law enforcement currently required to obtain a wiretap order since the unwitting victim system is not a "party to the communication" authorized to grant

consent to electronic surveillance? Would an exception to the wiretap law to allow the unwitting victim system operator to grant consent to electronic surveillance be helpful to law enforcement?

The question calls for an interpretation of a statute which would more appropriately be directed to the Department of Justice for a more detailed and definitive response. As a general matter, however, the FBI understands that: 1) the provisions of 18 U.S.C. §2511(1)(a) prohibit all interceptions unless expressly authorized elsewhere in the Act; 2) the provisions of 18 U.S.C. §2511(2)(a)(i) authorize a provider of wire or electronic communication services to intercept communications on their system, not because they are parties to those communications, but as "is a necessary incident to the rendition of [that] service or to the protection of the rights or property of the provider....;" 3) many providers (especially start-up Internet services) may not have the necessary tools or expertise to adequately track, document or halt an intruder in their system and, more perhaps more significantly, no providers have compulsory process to facilitate disclosure of transaction and subscriber information from other providers which is necessary to identify the source of an attack; 4) 18 U.S.C. §2511(2)(a)(i) does not permit law enforcement to conduct an interception (without a court order) even upon a provider's express request when the provider's system has been invaded or trespassed upon by a hacker, and 5) as a result of this quandary, and in order to ensure that evidence obtained will subsequently be held admissible, law enforcement is required to obtain a court order in order to enable it to actively work in conjunction with the provider.

Given the high level DOJ approval that is required for Title III Interception applications, the necessary generation of paperwork, and the time needed by the reviewing court, significant delay can occur before law enforcement can provide an effective response to a hacker or DDOS event. This anomaly in the law creates an untenable situation whereby providers are sometimes forced to sit idly by as they witness hackers enter and, in some situations, destroy or damage their systems and networks while law enforcement begins the detailed process of seeking court authorization to assist them. In the real world, the situation is akin to a homeowner being forced to helplessly watch a burglar or vandal while police seek a search warrant to enter the dwelling. For these reasons, the FBI favors enactment of a statutory exception under 18 U.S.C. §2511 which would expressly authorize law enforcement to assist such providers by intercepting the communications of a computer user/trespasser (the transmissions to and from the user/trespasser) BUT ONLY upon the voluntary, written consent of a service provider after that provider has made an initial determination that the user/trespasser is, in fact, not authorized to be on the system or network. Such an exception to the general interception prohibition would accelerate exponentially law enforcement's ability to respond to such hacker incidents and would be a significant step toward ensuring the security and integrity of the Nation's critical infrastructure.

1. Is law enforcement currently required to obtain a wiretap in order to document in real-time the remote commands being given to a target system?

potential exception to this would be certain pen register-based approaches employed by service providers in switch-based solutions, where post-cut-through dialing (including post-cut- through signaling) may not be provided to law enforcement. This circumstance is currently a subject of review by the FCC under rule making implementing CALEA, and regarding which we anticipate a resolution in the near future.) The distinction between a pen register device on a telephony service and a clone pager (or pager interception) is that a pen register is employed to capture dialed numbers which are used to set up a call. Hence, in the overwhelming majority of instances where pen registers are used the information captured is simply signaling information used to set up a call. By comparison, pager interceptions are employed to capture the information received by a pager which, in all instances, constitute the content or message of the call. Consequently, the law has historically distinguished the legal processes required for these two types of acquisitions (i.e., pen register authority vs Title III authority, respectively).

Pen register efforts in the data network area work somewhat differently. The most basic reason for this is because the services (e.g., email, web-based mail, voice over IP) and applications (e.g., Internet Chat, File Transfer) transmitted over data networks are somewhat different. Some of these services and applications lend themselves to precise ways of capturing (i.e., recording) call identifying and signaling information only while others make the process of differentiating signaling information from call content more difficult.

9(B) Section 3121(c) of title 18, United States Code, requires government agencies authorized to use pen registers to "use technology reasonably available...that restricts the recording or decoding of electronic or other impulses to the dialing and signaling information utilized in call processing." Please describe the technology and methodology currently employed to comply with this statutory requirement.

Pen Register devices on telephony services continue to operate as they have for decades. Stated differently, since the enactment of CALEA, there has been no change in technology or pen register equipment for telephony that would better restrict the recording or decoding of electronic or other impulses to the dialing and signaling information utilized in call processing.

As stated above, pen register efforts in the data network area work somewhat differently, and there, where technology that restricts the recording or decoding of electronic or other impulses to the dialing and signaling information is reasonably available, it is employed. For example, the FBI employs pen register devices to capture Internet Protocol (IP) addresses. Since data networks typically use well-established layered protocols, FBI tools are capable of restricting the information captured to the IP address.

10. Section 3121(a) of title 18, United States Code, requires a court to authorize the use of a pen register if the court finds that the government attorney has certified that the information likely to be obtained by "such use is relevant to an ongoing criminal investigation." The certification by the government attorney is, in turn, made under oath and penalty of perjury,

under section 3122.

(A) Is the government attorney required to describe to the court in the application for a pen register the factual basis for the attorney's certification that "such use is relevant to an ongoing criminal investigations"?

(B) As a matter of regular practice, do government attorneys or State law enforcement or investigative officers making applications for pen registers describe for the court the factual basis for the certification that "such use is relevant to an ongoing criminal investigation" or does this practice vary?

(C) What procedures, including audits or internal reviews, are in place to ensure that government attorneys and State law enforcement or investigative officers comply with the statutory standard and have the necessary factual basis for making the application, particularly in those districts where the practice in applying for pen register orders is not to describe for the court the factual basis for certification?

(D) Should the court, rather than governmental attorneys or State law enforcement or investigative officers, be given the authority to make the factual finding that "information likely to be obtained by such installation and use [of a pen register] is relevant to an ongoing criminal investigation," and if not, please explain why?

Several of the questions call for or implicate an interpretation of statute which would more appropriately be directed to the Department of Justice for a more detailed and definitive response. As a general matter, however, the FBI understands the Supreme Court has expressly ruled that "the installation of a pen register ...[is] not a "search" within the meaning of the Fourth Amendment and therefore its use does not violate the Constitution." Smith v. Maryland, 442 U.S. 735, 745-46, 99 S.Ct. 2577, 2583 (1979). Given the lack of an expectation of privacy at stake in the limited, non-content information garnered through the use of pen registers, the Courts have held that the limited judicial review role delineated by 18 U.S.C. §3121 *et seq.* is Constitutional and is intended to safeguard against the purely random use of pen register devices by ensuring compliance with the statutory requirements established by Congress. *See United States v. Hallmark*, 911 F.2d 399, 401-402 (10th Cir. 1990).

Pen Register certifications by government attorneys are drafted and filed by attorneys of the Department of Justice and not, at the Federal level, by Special Agents of the FBI. Questions regarding the substance of such certifications would more appropriately directed to the Department of Justice for a more definitive response. As a general matter, however, it is the FBI's experience that the degree to which a pen register application to the Court discloses the underlying factual basis for the attorney's certification turns, in large measure, upon the nature of the statutory offense which is the focus of the investigation. Whereas section 3123(b)(1)(D) requires that all pen register orders contain a "statement of the offense to which the information likely to be obtained by the pen register or trap and trace device relates," it follows that the application required by section 3122(b)(2) contain

such a statement within the attorney's certification and it is the FBI's experience that this is commonly the case. Depending upon the nature of the offense described in the certification, the underlying basis for the certification can, and in most instances will be readily apparent. Thus, in telemarketing fraud investigations, the obvious underlying basis is that the offenders are using the telephone to solicit victims. Similarly in narcotics and conspiracy to commit narcotics violations, the reliable and common sense inference is clearly that telecommunications are being used to facilitate the possession, distribution and sale of controlled substances in violation of Title 21 of the United States Code. Even in investigations involving computer hacking in violation of the Computer Fraud and Abuse Act (18 U.S.C. §§1030 *et seq.*), it requires little thought or imagination to understand the underlying basis for the request.

The FBI also understands that the sole basis for obtaining a pen register order is to further a criminal investigation by generating reliable admissible evidence. An attorney who falsely or recklessly certifies an application under oath pursuant to 18 U.S.C. §3122(b)(2) does so at his/her peril subject to sanction, disbarment and prosecution. Furthermore, an attorney who so falsely certifies such an application has no way of knowing the subsequent course and outcome of the investigation. Frequently, information received from a pen register is consolidated with other investigative information and is submitted in subsequent, more detailed applications to the Court such as search warrant applications or wiretap applications. In the unlikely event that an attorney for the government were to submit a false certification to the court in support of a pen register application, the lack of any nexus between the named subjects of the investigation, the "statement of the offense," and the attorney's certification that the information likely to be obtained from the devise's use is relevant to an ongoing criminal investigation would, in many instances, reveal itself either in subsequent applications to the Court for search warrants or wiretaps, or in discovery incident to prosecution. The dearth of such empirical or anecdotal evidence demonstrating inappropriate or false certification of applications by attorneys for the government demonstrates that the certification obligation is conscientiously fulfilled.

11. You have testified that information theft and financial fraud perpetrated online have caused the most severe financial losses, "put at $68 million and $56 million respectively." In fact, you have identified "use of the Internet for fraudulent purposes" as "one of the most critical challengers facing the FBI and law enforcement in general.: Appreciating this challenge, I have urged that the Congress be careful in considering legislation, such as H.R. 1714, " The Electronic Signatures in Global and National Commerce Act," to ensure that consumers are adequately protected in the online environment. This bill has passed the House of Representatives and is currently the subject of a conference with the Senate.

(A) The National Association of Attorneys General has commented on H.R. 1714, stating that the bill's provisions permitting storage of only synopses of documents that "accurately reflect" originals, even where the law otherwise requires retention of original documents, "has the strong potential to negatively impact law enforcement discovery of document." Do you agree and, if not, please explain why?

(B) H.R. 1714 would require that state enactments of the Uniform Electronic Transactions Act (UETA) "be consistent with" the House bill, resulting in federal preemption of any state exemption from the presumption of validity of electronic signatures and transactions that is not authorized in the House bill. The National Association of Attorneys General has opined that this broad federal preemption would "unduly hinder the ability of the states to protect their citizens against consumer fraud." If States are hindered in combating consumer fraud, would the FBI's job in protecting the public from fraudulent online practices be made more difficult?

On its face, the provisions of H.R. 1714 which allow for the electronic storage of contracts, agreements and records are unrelated to earlier provisions of the bill delineating what types of legal documents may be executed by electronic signature. To the extent that Section 101(c)(1)(c) could be interpreted as allowing for the electronic imaging and storage as an electronic record of written contracts or agreement, the tangible originals of which would otherwise be required by law to be maintained in tangible form, then, there could exist the potential to negatively impact certain law enforcement investigations relating to such documents. At a minimum, the supplanting of tangible originals (otherwise legally required to be maintained in tangible form) with electronic images depicting the originals, when coupled with destruction of the originals, would eliminate or complicate handwritten signature analysis and render null the possibility of recovering fingerprints or other trace evidence from the surface of originals. By the same token, the provisions of section 101(c)(2) which exempt from retention data relating to the communication or receipt of any contract, agreement or record electronically recorded, could, in the context of electronically executed contracts, complicate or eliminate law enforcement efforts in tracing the source of transmission of fraudulent transactions or the location and identity of co-conspirators or even other victims. The continued trend toward electronic, paper-less execution of commercial transactions (which is admittedly so critical to the continued evolution and expansion of the Internet) when coupled with 1) the growing ability of criminals to utilize encryption to restrict law enforcement's ability to recover crucial inculpatory evidence, and 2) the absence of any preeminent public key, or private signature verification entity or procedure complicates the efforts of the FBI and state law enforcement to protect the public from on-line fraud.

1. synopses only of documents can negatively impact law enforcement?

The review of complete and accurate records is often necessary in law enforcement's effort to help investigate crime. All records management and retention policies therefore can be said to have an effect on law enforcement, and those policies which do not require that information be maintained, at least in theory, can negatively impact law enforcement's discovery of that information.

2. If states are hindered . . .

The FBI believes that since States are the primary responders to crime in our country, if the States are hindered in combating consumer fraud, then the FBI's job in protecting the public from fraudulent online practices wold be made more difficult.

Citation Search Result Rank 4 of 18 Database
U.S. Attys. Man. 9-7.010 USAM
U.S. Attorney's Manual 9-7.010

TEXT

UNITED STATES DEPARTMENT OF JUSTICE
UNITED STATES ATTORNEYS MANUAL
TITLE 9-CRIMINAL
CHAPTER 9-7.000 ELECTRONIC SURVEILLANCE
September 1997

9-7.010 Introduction

This chapter contains Department of Justice policy on the use of electronic surveillance. The Federal electronic surveillance statutes (commonly referred to collectively as "Title III") are codified at 18 U.S.C. § 2510, et seq. Because of the well-recognized intrusive nature of many types of electronic surveillance, especially wiretaps and "bugs," and the Fourth Amendment implications of the government's use of these devices in the course of its investigations, the relevant statutes (and related Department of Justice guidelines) provide restrictions on the use of most electronic surveillance, including the requirement that a high-level Department official specifically approve the use of many of these types of electronic surveillance prior to an Assistant United States Attorney obtaining a court order authorizing interception.

Chapter 7 contains the specific mechanisms, including applicable approval requirements, for the use of wiretaps, "bugs" (oral interception devices), roving taps, video surveillance, and the consensual monitoring of wire or oral communications, as well as emergency interception procedures and restrictions on the disclosure and evidentiary use of information obtained through electronic surveillance. Additional information concerning use of the various types of electronic surveillance is also set forth in the Criminal Resource Manual at 27.

Attorneys in the Electronic Surveillance Unit of the Office of Enforcement Operations, Criminal Division, are available to provide assistance concerning both the interpretation of Title III and the review process necessitated thereunder. Interceptions conducted pursuant to the Foreign Intelligence Surveillance Act of 1978, which is codified at 50 U.S.C. § 1801, et seq., are specifically excluded from the coverage of Title III. See 18 U.S.C. § 2511(2)(a)(ii), (2)(e), and (2)(f).

9-7.010
U.S. Attys. Man. 9-7.010
END OF DOCUMENT

DOC #15

Citation Search Result Rank 5 of 18 Databas
U.S. Attys. Man. 9-7.100 USAM
U.S. Attorney's Manual 9-7.100

TEXT

UNITED STATES DEPARTMENT OF JUSTICE
UNITED STATES ATTORNEYS MANUAL
TITLE 9-CRIMINAL
CHAPTER 9-7.000 ELECTRONIC SURVEILLANCE
September 1997

9-7.100 Authorization of Applications for Wire, Oral, and Electronic Interception Orders--Overview and History of Legislation

To understand the core concepts of the legislative scheme of Title III, one must appreciate the history of this legislation and the goals of Congress in enacting this comprehensive law. By enacting Title III in 1968, Congress prohibited private citizens from using certain electronic surveillance techniques. Congress exempted law enforcement from this prohibition, but required compliance with explicit directives that controlled the circumstances under which law enforcement's use of electronic surveillance would be permitted Many of the restrictions upon the use of electronic surveillance by law enforcement agents were enacted in recognition of the strictures against unlawful searches and seizures contained in the Fourth Amendment to the United States Constitution. See, e.g., Katz v. United States, 389 U.S. 347 (1967). Still, several of Title III's provisions are more restrictive than what is required by the Fourth Amendment. At the same time, Congress preempted State la in this area, and mandated that States that sought to enact electronic surveillance laws would have to make their laws at least as restrictive as the Federal law.

One of Title III's most restrictive provisions is the requirement that Federal investigative agencies submit requests for the use of certain types of electronic surveillance (primarily the non-consensual interception of wire and oral communications) to the Department of Justice for review and approval before applications for such interception may be submitted to a court of competent jurisdiction for an order authorizing the interception. Specifically, in 18 U.S.C. § 2516(1), Title III explicitly assigns such review and approval powers to the Attorney General, but allows the Attorney General to delegate this review and approval authority to a limited number of high-level Justice Department officials, including Deputy Assistant Attorneys General for the Criminal Division ("DAAGs"). The DAAGs review and approve or deny proposed applications to conduct "wiretaps" (to intercept wire [telephone] communications, 18 U.S.C. § 2510(1)) and to install and monitor "bugs" (the use of microphones to intercept oral [face-to-face] communications, 18 U.S.C. § 2510(2)). It should be noted that only those crimes enumerated in 18 U.S.C. § 2516(1) may be investigated through the interception of wire or oral communications. On those rare occasions when the government seeks to intercept oral or wire communications within premises or over a facility that cannot be identified with any particularity, and a "roving" interception of wire or oral communications is therefore being requested, the Assistant Attorney General or the Acting Assistant Attorney

U.S. Attys. Man. 9-7.100

TEXT
General for the Criminal Division must be the one to review and approve or deny the application. (See the roving interception provision at 18 U.S.C. § 2518(11), discussed at USAM 9-7.111.)

In 1986, Congress amended Title III by enacting the Electronic Communications Privacy Act of 1986. Specifically, Congress added a new category of covered communications, i.e., "electronic communications," which would now be protected, and whose interception would be regulated, by Title III. Electronic communications are those types of non-oral or wire communications that occur, inter alia, over computers, digital-display pagers, and facsimile ("fax") machines. See 18 U.S.C. § 2510(12).

Although the 1986 amendments permit any government attorney to authorize the making of an application to a Federal court to intercept electronic communications to investigate any Federal felony (18 U.S.C. § 2516(3)), the Department of Justice and Congress agreed informally at the time of ECPA's enactment that, for a three-year period, Department approval would nonetheless be required before applications could be submitted to a court to conduct interceptions of electronic communications. After that period, the Department rescinded the prior approval requirement for the interception of electronic communications over digital-display paging devices, but continued the need for Department approval prior to application to the court for the interception of electronic communications over any other device, such as computers and fax machines. Applications to the court for authorization to intercept electronic communications over digital-display pagers--which are the most commonly targeted type of electronic communications--may be made based solely upon the authorization of a United States Attorney. See 18 U.S.C. § 2516(3).

Because there are severe penalties for the improper and/or unlawful use and disclosure of electronic surveillance evidence, including criminal, civil, and administrative sanctions, as well as the suppression of evidence, it is essential that Federal prosecutors and law enforcement agents clearly understand when Departmental review and approval are required, and what such a process entails. See 18 U.S.C. §§ 2511, 2515, 2518(10), and 2520.

See the Criminal Resource Manual at 31, for citations to relevant legislation.

9-7.100
U.S. Attys. Man. 9-7.100
END OF DOCUMENT

Citation Search Result Rank 6 of 18 Database
U.S. Attys. Man. 9-7.110 USAM
U.S. Attorney's Manual 9-7.110

TEXT

UNITED STATES DEPARTMENT OF JUSTICE
UNITED STATES ATTORNEYS MANUAL
TITLE 9-CRIMINAL
CHAPTER 9-7.000 ELECTRONIC SURVEILLANCE
September 1997

9-7.110 Format for the Authorization Request

When Justice Department review and approval of a proposed application for electronic surveillance is required, the Electronic Surveillance Unit of the Criminal Division's Office of Enforcement Operations will conduct the initial review of the necessary pleadings, which include:

A. The affidavit of an "investigative or law enforcement officer" of the United States who is empowered by law to conduct investigations of, or to make arrests for, offenses enumerated in 18 U.S.C. § 2516(1) or (3) (which, for any application involving the interception of electronic communications, includes any Federal felony offense), with such affidavit setting forth the facts of the investigation that establish the basis for those probable cause (and other) statements required by Title III to be included in the application;

B. The application by any United States Attorney or his/her Assistant, or any other attorney authorized by law to prosecute or participate in the prosecution of offenses enumerated in 18 U.S.C. § 2516(1) or (3) that provides the basis for the court's jurisdiction to sign an order authorizing the requested interception of wire, oral, and/or electronic communications; and

C. A set of orders to be signed by the court authorizing the government to intercept, or approving the interception of, the wire, oral, and/or electronic communications that are the subject of the application, including appropriate redacted orders to be served on any relevant providers of "electronic communication service" (as defined in 18 U.S.C. § 2510(15)).

9-7.110
U.S. Attys. Man. 9-7.110
END OF DOCUMENT

Citation Search Result Rank 16 of 18 Database
U.S. Attys. Man. 9-60.202 USAM
U.S. Attorney's Manual 9-60.202

TEXT

UNITED STATES DEPARTMENT OF JUSTICE
UNITED STATES ATTORNEYS MANUAL
TITLE 9-CRIMINAL
CHAPTER 9-60.000 PROTECTION OF THE INDIVIDUAL
September 1997

9-60.202 Illegal Electronic Eavesdropping--Prosecution Policy

The criminal prohibitions against illegal electronic eavesdropping contained in Title III are part of the same act which permits federal law enforcement officers to engage in court-authorized electronic surveillance. Congress viewed the criminal sanctions and the court authorization provisions as two sides of the same coin. The retention of the government's authorization to engage in court-authorized electronic surveillance may depend on its vigorous enforcement of the sanctions against illegal electronic eavesdropping. Accordingly, it is the Department's policy to vigorously enforce these criminal prohibitions.

The Department's overall prosecutive policy under 18 U.S.C. $ 2511 is to focus primarily on persons who engage or procure illegal electronic surveillance as part of the practice of their profession or as incident to their business activities. Less emphasis should be placed on the prosecution of persons who, in the course of transitory situations, intercept communications on their own without the assistance of a professional wiretapper or eavesdropper. This does not mean that such persons are never to be prosecuted, but simply that this type of prosecution is not a major thrust of the Department's enforcement program.

Most illegal interceptions fall into one of five categories: (1) domestic relations, (2) industrial espionage, (3) political espionage, (4) law enforcement, and (5) intra-business. The largest number of interceptions, more than 75 percent, are in the domestic relations category. It is the Department's policy to vigorously investigate and prosecute illegal interceptions of communications which fall within the industrial and political espionage, law enforcement, and intra-business categories. Generally such violations will have interstate ramifications which will make federal prosecution preferable to state prosecution. Nevertheless, in cases where the federal interest is slight, it may be appropriate to defer to state prosecution.

Illegal interceptions arising from domestic relations disputes generally present less of a federal interest and, therefore, local prosecution is more appropriate. However, this does not mean that federal prosecutors should abdicate responsibility for prosecuting such interceptions. Indeed, in view of the preponderance of this kind of interception, no enforcement program can be effective without the initiation of some prosecutions for deterrence purposes. United States Attorneys should develop effective liaison with local prosecutors in order to convince them to shoulder their share of the burden.

Within the category of domestic relations violations, primary attention should be given to those instances in which a professional is involved, such as a private detective, attorney, moonlighting telephone company employee, and

TEXT
supplier of electronic surveillance devices. United States Attorneys should feel free to pursue these cases or refer them to local prosecutors; however, no professional should escape prosecution when a prosecutable case exists.

Domestic relations violations which do not involve a professional interceptor are the lowest priority cases for federal prosecution. Although local prosecution is normally preferable, when local prosecutors are unwilling to pursue the case, resort to federal prosecution may be appropriate. Nevertheless, violations of this type will sometimes prove to be of insufficient magnitude to warrant either federal or state prosecution. In such cases, other measures may prove sufficient, for example, a civil suit for damages (18 U.S.C. § 2520), suppression of evidence (18 U.S.C. § 2515), or forfeiture of the wiretapping or eavesdropping paraphernalia (18 U.S.C. § 2513).

Disturbed persons often suspect that they are the victims of illegal interceptions. Consequently, a complaint which is based solely on suspicious noises heard on the telephone normally does not merit further investigation if the initial line check fails to produce independent evidence of a tap.

9-60.202
U.S. Attys. Man. 9-60.202
END OF DOCUMENT

Citation Search Result Rank 17 of 18 Database
U.S. Attys. Man. 9-60.262 USAM
U.S. Attorney's Manual 9-60.262

TEXT

UNITED STATES DEPARTMENT OF JUSTICE
UNITED STATES ATTORNEYS MANUAL
TITLE 9-CRIMINAL
CHAPTER 9-60.000 PROTECTION OF THE INDIVIDUAL
September 1997

9-60.262 Prosecutive Policy--18 U.S.C. § 2512

Flagrant violators of 18 U.S.C. § 2512 should be prosecuted vigorously, especially violators who possess such devices in order to engage in electronic surveillance as a business.

Less culpable first offenders and those who violate the statute because of ignorance of the law may be appropriate subjects for more lenient disposition. In some cases a warning may be sufficient. Nevertheless, in all cases except, perhaps, for minor advertising violations, the United States Attorney's Office should require that the prohibited device either be surrendered voluntarily to the FBI or forfeited pursuant to 18 U.S.C. § 2513.

9-60.262
U.S. Attys. Man. 9-60.262
END OF DOCUMENT

b6-1 / b7c-1

From: [redacted] b6-1
To: [redacted] b7c-1
Date: 7/20/00 6:20PM
Subject: Don Kerr's Testimony

b6-1
b7c-1 [redacted]

The revisions that I just gave you do not include a fix for the problem that we just discussed, namely, the difference between T-III's standards for interception of oral/wire communications, and those for electronic communications. The former are set forth in 18 USC 2516(1), the latter in 18 USC 2516(3).

For the purpose of this testimony, the two main differences are:
(1) that applications under 2516(3) do not require senior level DOJ approval and (2) that they are not limited to "certain federal felonies. Thus if we strike the sentence at the bottom of page two/top of page three (referring to authorization by a senior official of DOJ) and the last sentence in the first paragraph of page three ("Further, interception of communications is limited to certain specified felony offenses.") we will remove some of the misleading inferences as to which provision we follow when seeking court approval to intercept e-mail. There may may be other instances where the testimony suggests that we use 2616(1) rather than 2516(3); OGC should scrub the testimony again to check for such instances.

[redacted]

b6-1
b7c-1

CC: [redacted] CHARLES STEELE [redacted] b6-1 b7c-1

Doc. #16

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

25 Pages were not considered for release as they are duplicative of DOCUMENT #13, OGC FRONT OFFICE FILE (PGS 20-44)

_____ Page(s) withheld for the following reason(s): _____

☒ The following number is to be used for reference regarding these pages:
DOCUMENT #17 (Pages 420-444)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

Doc. #18

IP Addresses

Example: 192.16.201.10

(Like a phone number)

Identifies a specific computer

How is Data Sent?

Example Email:

To: Jdoe@erols.com
From: JaneD@freedomnet.com
Subject: Blah

Hey John,
Blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah blah
...

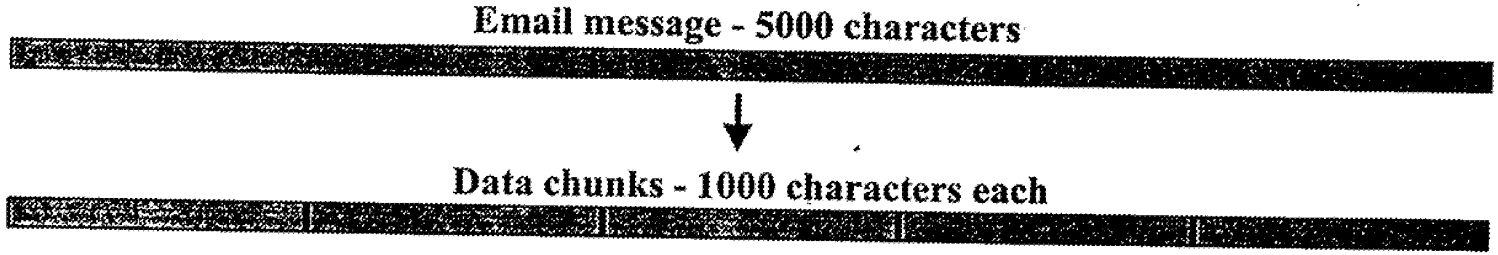
↓

To: Jdoe@erols.com~~From: JaneD@freedomnet.com~~Subject: Blah~~Hey John,~~ Blah blah blah blah blah blah blah blah blah

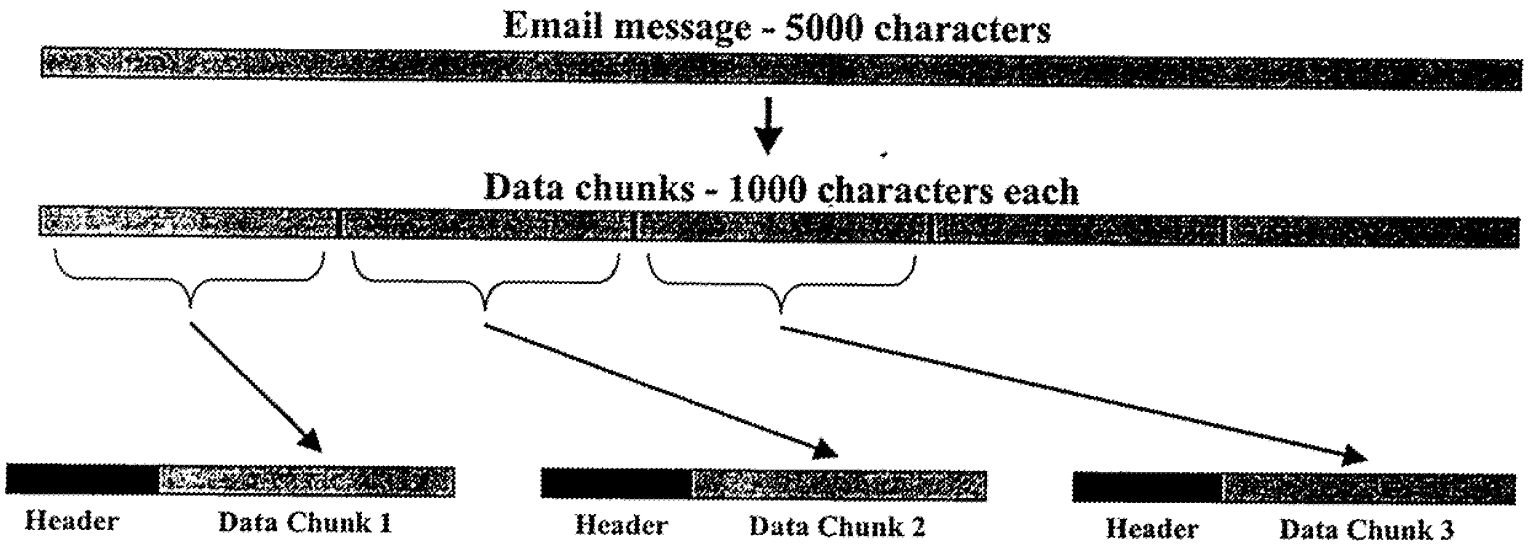
How is Data Sent?

Email message - 5000 characters

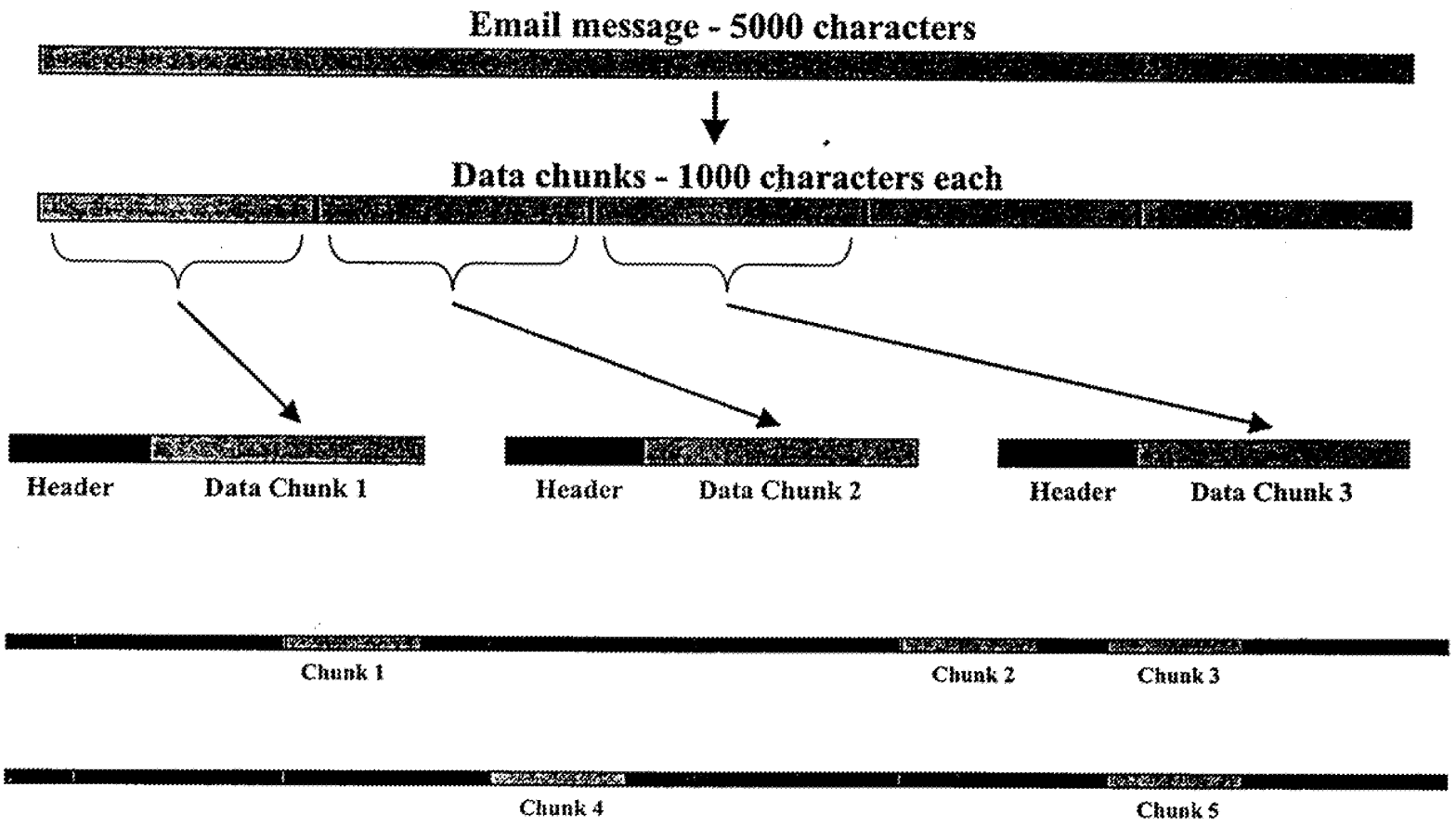
How is Data Sent?



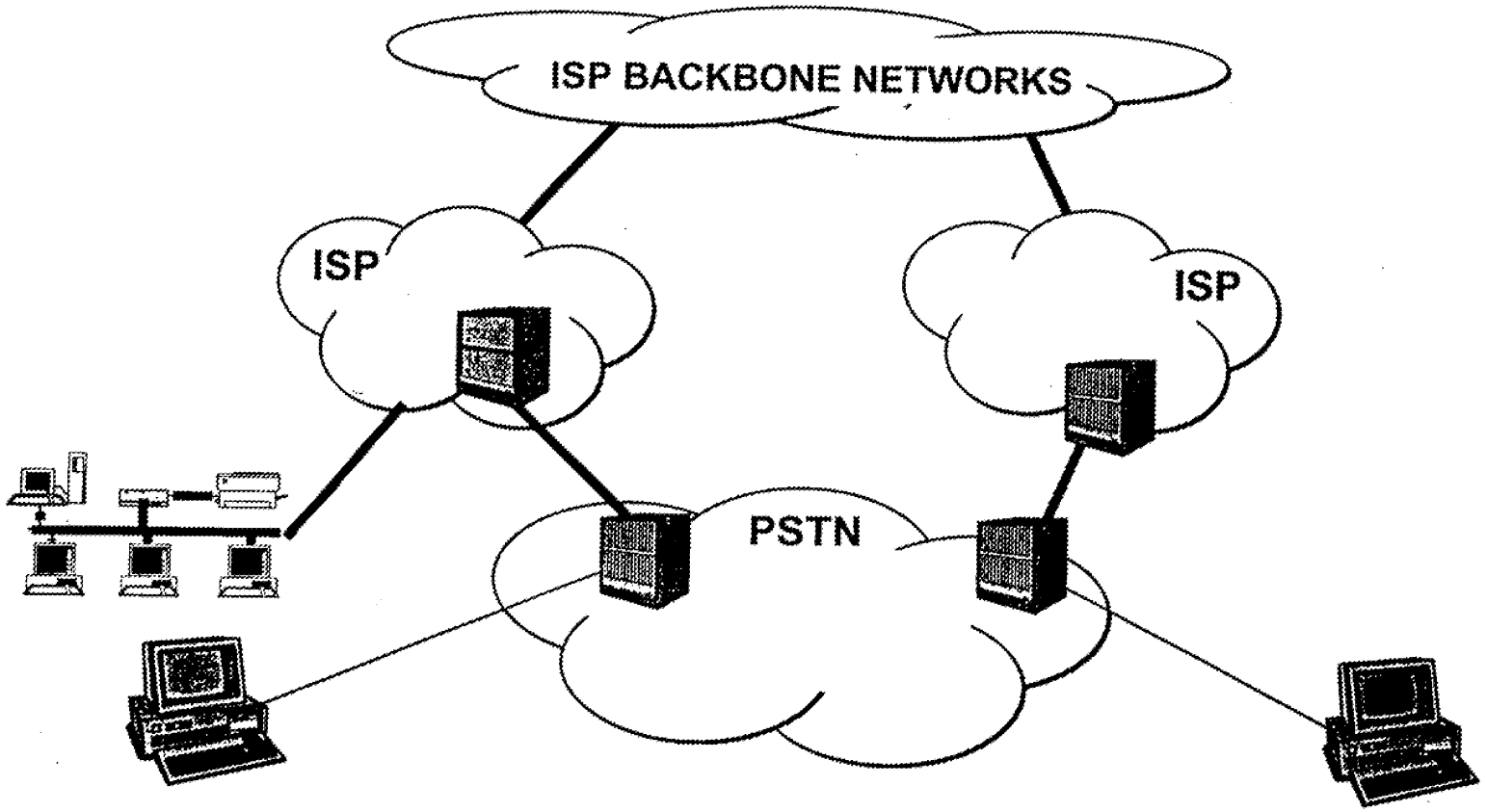
How is Data Sent?

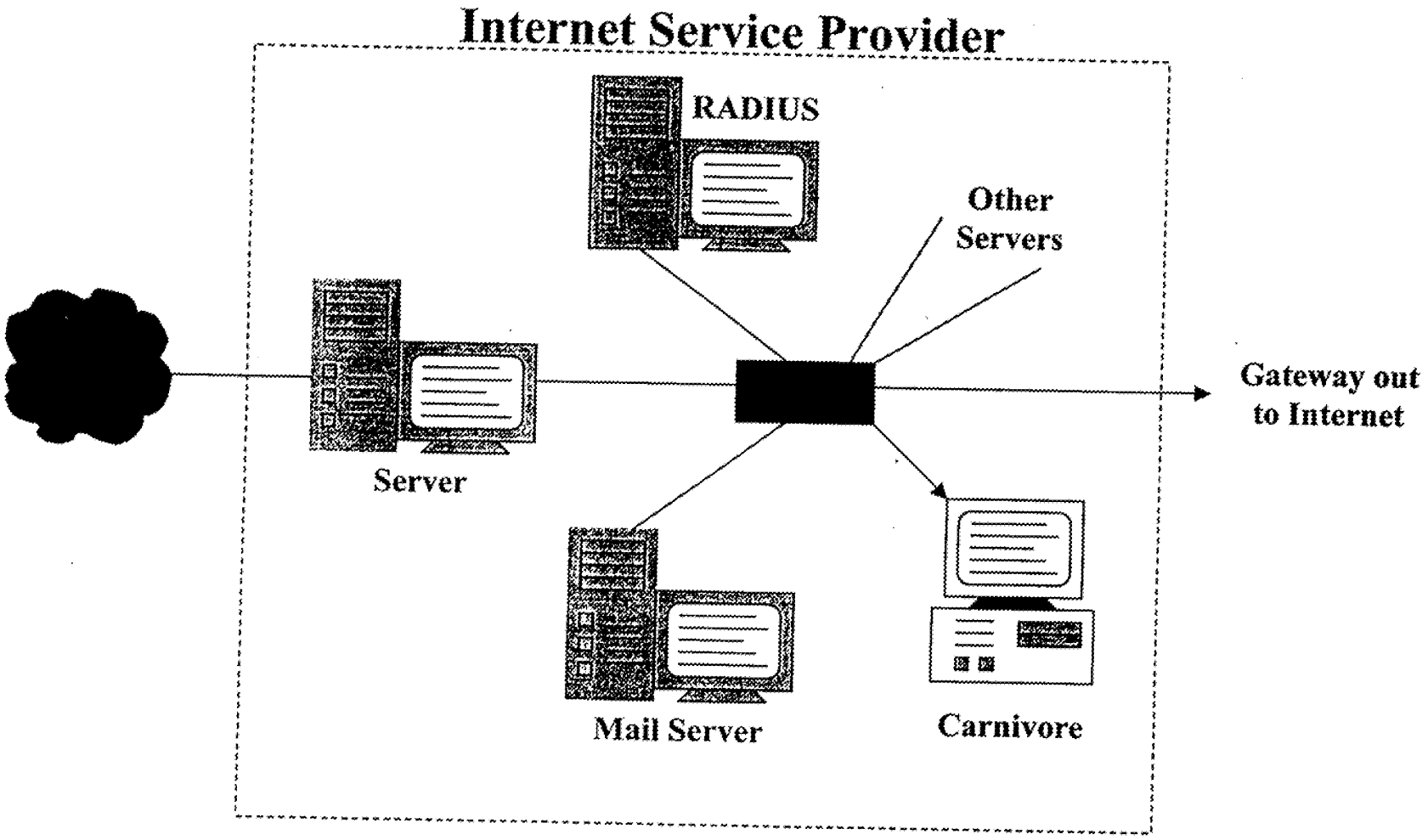


How is Data Sent?



Network Schematic




Internet Service Provider
RADIUS
Other Servers
Server
Gateway out to Internet
Mail Server
Carnivore

b6-1/b7c-1

b6-1
b7c-1

From: [redacted]
To: LARRY PARKINSON
Subject: Carnivore

b6-1
b7c-1

b6-1
b7c-1

(703) [redacted]

Larry: I wanted to bring you up to date re: Carnivore. I am leaving for Denver this morning to attend a Health Care Fraud Conference. I have brought [redacted] up to speed and he will be assiting you, OPCA and the Lab this week. There is one briefing scehdule with the Intelligence Committee on Wednesday, 7/19 at 10:00am. [redacted] will be going with [redacted] (OPCA) and [redacted] I was advised that next week there will be House hearings and that Dr. Kerr and you will be testifying. How [redacted] explained it to me was Dr.Kerr will read an opening statement that will incorporate both the technical aspects of Carnivore and the legal authority for its use. If this meets with your approval, both [redacted] and [redacted] will write the statement.

Carnivore is a sotware package that can be installed in box that can easily blend with other devices located at an ISP. It is only used under court order; it is not a continous running system. The software is maintianed at Quantico and is sent to a field office when needed. It was developed by us because we were not able to diferentiate between customers and/or messages. Jugdes were authorizing very narrow intercepts and we needed the ability to narrow our interception up front rather that with post-minimization. Carnivore "sniffs" up front and captures only those e-mails we are authorized to intercept or wnat to intercept.

How does it do this? It does this though a series of filters. The filters allow you to exclude those e-mails you do not want. As an example - the subject of your case is represented by counsel and communictes with him via e-mail. You can program Carnivore so that you will not capture these e-mails. Or you wnat to capture someone'e Web mail but not all his Web traffic (i.e. his brousing through catalogues shopping). Carnivore can limit the intercepts just to web mail. Therefore, it is actaully a privacy protector not invador.

Data is not stored on the Canivore device. It is stored on a disc or zip-drve that is locked by key by the agent and removed only by the agent so as to maintian chain of custody. The disc is then brought back to the field office and placed into a reading device. There is an additional minimization step that occurs at the field office to ensure that the case agent does not read any e-mails that he is not authorize to use pursuant to the court order. We may have information up front that allows us to filter e-mails but there may be times that we determine throught the course of the intercept that there are e-mails we can't have. Since most of our Carnivore intercepts are not real time, we need to post minimize. Once we learn that there is e-mail traffic we do not want, we can go back to the device and add filters to the program so that we will not capture the e-mails again.

I attended two briefings last week. One was with the Judiciary Committee minority staffers. They seemed more interested in understanding how Carnivore works, how long we have been using it, for what types of cases and were quite content once they learned that we only use Carnivore pursuant to a court order. They seemed quite satisfied with the briefing.

CC: CHARLES STEELE, [redacted]

b6-1
b7c-1

"Shall" to "may"

IP address / Scope of phone #?

Signaling

Clearer language -

Additional subpoena for Pen order

Doc #19

WALL STREET JOURNAL

DATE 7/11/00
PAGE A3

FBI's Wiretaps To Scan E-Mail Spark Concern

By Neil King Jr.
And Ted Bridis
Staff Reporters of The Wall Street Journal

WASHINGTON—The Federal Bureau of Investigation is using a superfast system called Carnivore to covertly search e-mails for messages from criminal suspects.

Essentially a personal computer stuffed with specialized software, Carnivore represents a new twist in the federal government's fight to sustain its snooping powers in the Internet age. But in employing the system, which can scan millions of e-mails a second, the FBI has upset privacy advocates and some in the computer industry. Experts say the system opens a thicket of unresolved legal issues and privacy concerns.

The FBI developed the Internet wiretapping system at a special agency lab at Quantico, Va., and dubbed it Carnivore for its ability to get to "the meat" of what would otherwise be an enormous quantity of data. FBI technicians unveiled the system to a roomful of astonished industry specialists here two weeks ago in order to steer efforts to develop standardized ways of complying with federal wiretaps. Federal investigators say they have used Carnivore in fewer than 100 criminal cases since its launch early last year.

Word of the Carnivore system has disturbed many in the Internet industry because, when deployed, it must be hooked directly into Internet service providers' computer networks. That would give the government, at least theoretically, the ability to eavesdrop on all customers' digital communications, from e-mail to online banking and Web surfing.

The system also troubles some Internet service providers, who are loath to see outside software plugged into their systems. In many cases, the FBI keeps the secret Carnivore computer system in a locked cage on the provider's premises, with agents making daily visits to retrieve the data captured from the provider's network. But legal challenges to the use of Carnivore are few, and judges' rulings remain sealed because of the secretive nature of the investigations.

Internet wiretaps are conducted only under state or federal judicial order, and occur relatively infrequently. The huge majority of wiretaps continue to be the traditional telephone variety, though U.S. officials say the use of Internet eavesdropping is growing as everyone from drug dealers to potential terrorists begins to conduct business over the Web.

SUBJECT: The FBI's e-mail tapping system, Carnivore.
TO: The computer industry
FROM: The FBI

1. The FBI installs one of its off-the-shelf PCs at the Internet service provider of the surveillance target.
2. The PC checks e-mails passing through the ISP for information that indicates whether an e-mail is going to or from the target.
3. If it is, the PC copies the full text of the e-mail to the PC's removable hard drive, which an FBI agent collects daily.
4. While it does analyze the destination and sender of other e-mails, Carnivore does not retrieve their full text.
5. Once the surveillance ends (average 45 days), an FBI agent gathers the computer from the ISP.

The FBI defends Carnivore as more precise than Internet wiretap methods used in the past. The bureau says the system allows investigators to tailor an intercept operation so they can pluck only the digital traffic of one person from among the stream of millions of other messages. An earlier version, aptly code-named Omnivore, could suck in as much as to six gigabytes of data every hour, but in a less discriminating fashion.

Still, critics contend that Carnivore is open to abuse.

Mark Rasch, a former federal computer-crimes prosecutor, said the nature of the surveillance by Carnivore raises important privacy questions, since it analyzes part of every snippet of data traffic that flows past, if only to determine whether to record it for police.

"It's the electronic equivalent of listening to everybody's phone calls to see if it's the phone call you should be monitoring," Mr. Rasch said. "You develop a tremendous amount of information."

Others say the technology dramatizes how far the nation's laws are lagging behind the technological revolution. "This is a clever way to use old telephone-era statutes to meet new challenges, but clearly there is too much latitude in the current law," said Stewart Baker, a lawyer specializing in telecommunications and Internet regulatory matters.

Robert Corn-Revere, of the Hogan & Hartson law firm here, represented an unidentified Internet service provider in one of the few legal fights against Carnivore. He said his client worried that the FBI would have access to all the e-mail traffic on its system, raising dire privacy and security concerns. A federal magistrate ruled against the company early this year, leaving it no option but to allow the FBI access to its system.

"This is an area in desperate need of clarification from Congress," said Mr. Corn-Revere.

"Once the software is applied to the ISP, there's no check on the system," said Rep. Bob Barr, R-Ga., who sits on a House judiciary subcommittee for constitutional affairs. "If there's one word I would use to describe this, it would be 'frightening.'"

Marcus Thomas, chief of the FBI's Cyber Technology Section at Quantico, said Carnivore represents the bureau's effort to keep abreast of rapid changes in Internet communications while still meeting the rigid demands of federal wiretapping statutes. "This is just a very specialized sniffer," he said.

He also noted that criminal and civil penalties prohibit the bureau from placing unauthorized wiretaps, and any information gleaned in those types of criminal cases would be thrown out of court. Typical Internet wiretaps last around 45 days, after which the FBI removes the equipment. Mr. Thomas said the bureau usually has as many as 20 Carnivore systems on hand, "just in case."

FBI experts acknowledge that Carnivore's monitoring can be stymied with computer data such as e-mail that is scrambled using powerful encryption technology. Those messages still can be captured, but law officers trying to read the contents are "at the mercy of how well it was encrypted," Mr. Thomas said.

Most of the criminal cases where the FBI used Carnivore in the past 18 months focused on what the bureau calls "infrastructure protection," or the hunt for hackers, though it also was used in counterterrorism and some drug-trafficking cases.

DOC. #20

ADDITIONAL CARNIVORE DOCUMENTS

FROM

OFFICE OF PUBLIC AND CONGRESSIONAL AFFAIRS (THROUGH 7/28/00)

PAGES REVIEWED: 49

PAGES RELEASED: 49

EXEMPTIONS CITED: NONE

NOTE: 57 pages from this file are duplicates to pages from The Office of General Counsel's Front Office file, The Office of General Counsel's/Technology Law Unit (TLU) file and The Office of General Counsel's/ Investigative Law Unit (ILU) file.

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552

☐ (b)(1)
☐ (b)(2)
☐ (b)(3)
_____
_____
_____
☐ (b)(4)
☐ (b)(5)
☐ (b)(6)
☐ (b)(7)(A)
☐ (b)(7)(B)
☐ (b)(7)(C)
☐ (b)(7)(D)
☐ (b)(7)(E)
☐ (b)(7)(F)
☐ (b)(8)
☐ (b)(9)

Section 552a

☐ (d)(5)
☐ (j)(2)
☐ (k)(1)
☐ (k)(2)
☐ (k)(3)
☐ (k)(4)
☐ (k)(5)
☐ (k)(6)
☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

1 Pages were not considered for release as they are duplicative of DOC #20, OGC/INVESTIGATIVE LAW UNIT FILE (Pg. 453

_____ Page(s) withheld for the following reason(s): _____

X The following number is to be used for reference regarding these pages:
DOCUMENT #1 (Page 456)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552

☐ (b)(1)
☐ (b)(2)
☐ (b)(3)
_____
_____
_____
☐ (b)(4)
☐ (b)(5)
☐ (b)(6)
☐ (b)(7)(A)
☐ (b)(7)(B)
☐ (b)(7)(C)
☐ (b)(7)(D)
☐ (b)(7)(E)
☐ (b)(7)(F)
☐ (b)(8)
☐ (b)(9)

Section 552a

☐ (d)(5)
☐ (j)(2)
☐ (k)(1)
☐ (k)(2)
☐ (k)(3)
☐ (k)(4)
☐ (k)(5)
☐ (k)(6)
☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

3 Pages were not considered for release as they are duplicative of DOC #1, OGC/TECHNOLOGY LAW UNIT FILE (PAGES 155-157)

_____ Page(s) withheld for the following reason(s): _____

X The following number is to be used for reference regarding these pages:
DOCUMENT #2 (Pages 457-459)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

Want to send this story to another AOL member? Click on the heart at the top of this window.

FBI e-mail Snooping Device Attacked

By D. IAN HOPPER
.c The Associated Press

WASHINGTON (AP) - Civil liberties and privacy groups are railing against a new system designed to allow law enforcement agents to intercept and analyze huge amounts of e-mail in connection with an investigation.

The system, called "Carnivore," was first hinted at on April 6 in testimony to a House subcommittee. Now the FBI has it in use.

When Carnivore is placed at an Internet service provider, it scans all incoming and outgoing e-mails for messages associated with the target of a criminal probe.

In a letter addressed to two members of the House subcommittee that deals with Fourth Amendment search-and-seizure issues, the American Civil Liberties Union argued that the system breaches the Internet provider's rights and the rights of all its customers by reading both sender and recipient addresses, as well as subject lines of e-mails, to decide whether to make a copy of the entire message.

Further, while the system is plugged into the Internet provider's systems, it is controlled solely by the law enforcement agency. In a traditional wiretap, the tap is physically placed and maintained by the telephone company.

"Carnivore is roughly equivalent to a wiretap capable of accessing the contents of the conversations of all of the phone company's customers, with the 'assurance' that the FBI will record only conversations of the specified target," read the letter. "This 'trust us, we are the government' approach is the antithesis of the procedures required under our wiretapping laws."

Barry Steinhardt, associate director of the ACLU, said citizens shouldn't trust that such a sweeping data-tap will only be used against criminal suspects. And even then, he said, the data mined by Carnivore, particularly subject lines, are already intrusive.

"Law enforcement should be prohibited from installing any device that allows them to intercept communications from persons other than the target," Steinhardt said in an interview. "When conducting these kinds of investigations, the information should be restricted to only addressing information."

A spokeswoman for Rep. Charles T. Canady, R-Fla., who heads the House Judiciary subcommittee on the Constitution, said the congressman had no comment on the letter.

In testimony to Canady's subcommittee, Robert Corn-Revere, a lawyer at the Hogan & Hartson law firm in Washington, said he represented an Internet provider that refused to install the Carnivore system. The provider was placed in an "awkward position," Corn-Revere said, because the company feared suits from customers unhappy with the government looking into all the e-mail.

"It was acknowledged (by the government) that Carnivore would enable remote access to the ISP's network and would be under the exclusive control of government agents," Corn-Revere said.

Corn-Revere told the committee that current law is insufficient to deal with Carnivore's potential and that the Internet provider lost its court battle in part because of the Internet's connection to telephone lines, and that the law was stretched to cover the Internet as well.

Corn-Revere would not reveal the name of his client, and the client lost the case. He said the FBI has been using Carnivore since early this year.

James X. Dempsey, senior staff counsel at the Center for Democracy and Technology, said the main problem with Carnivore is its mystery.

"The FBI is placing a black box inside the computer network of an ISP," Dempsey said. "Not even the ISP knows exactly what that gizmo is doing."

But Dempsey said Internet providers contributed to the problem, by saying that current technology does not allow the Internet provider to sort out exactly what the government is entitled to get under a search warrant. The carriers complained that they had to give everything to the FBI.

"The service providers said they didn't know how to comply with court orders," Dempsey said. "By taking that position, they have hurt themselves, putting themselves into a box."

Marcus Thomas, who heads the FBI's cybertechnology section, told the Wall Street Journal that the bureau has about 20 Carnivore systems, which are PCs with proprietary software. He said Carnivore meets current wiretapping laws, but is designed to keep up with the Internet.

"This is just a specialized sniffer," Thomas told the Journal, which first reported details about Carnivore.

Encrypted e-mail, done with an e-mail encoding program like PGP, still stays in code on Carnivore, and it's up to agents to decode it.

Dempsey has a possible solution to the problem, though one that's probably unlikely - show everyone what it does and how it does it, allowing Internet providers to install the software themselves.

"The FBI should make this gizmo an open-source product," he said. "Then the secret is gone."

On the Net: Federal Bureau of Investigation: http://www.fbi.gov

American Civil Liberties Union: http://www.aclu.org

Center for Democracy and Technology: http://www.cdt.org

Pretty Good Privacy (PGP): www.pgp.com

AP-NY-07-12-00 0812EDT

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552

☐ (b)(1)
☐ (b)(2)
☐ (b)(3)
_____
_____
_____
☐ (b)(4)
☐ (b)(5)
☐ (b)(6)
☐ (b)(7)(A)
☐ (b)(7)(B)
☐ (b)(7)(C)
☐ (b)(7)(D)
☐ (b)(7)(E)
☐ (b)(7)(F)
☐ (b)(8)
☐ (b)(9)

Section 552a

☐ (d)(5)
☐ (j)(2)
☐ (k)(1)
☐ (k)(2)
☐ (k)(3)
☐ (k)(4)
☐ (k)(5)
☐ (k)(6)
☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

1 Pages were not considered for release as they are duplicative of Doc #2, OGC FRONT OFFICE FILE (PAGE 2)

_____ Page(s) withheld for the following reason(s): _____

X The following number is to be used for reference regarding these pages:
DOCUMENT #4 (Page 462)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DO

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552

☐ (b)(1)
☐ (b)(2)
☐ (b)(3)
_____
_____
_____
☐ (b)(4)
☐ (b)(5)
☐ (b)(6)
☐ (b)(7)(A)
☐ (b)(7)(B)
☐ (b)(7)(C)
☐ (b)(7)(D)
☐ (b)(7)(E)
☐ (b)(7)(F)
☐ (b)(8)
☐ (b)(9)

Section 552a

☐ (d)(5)
☐ (j)(2)
☐ (k)(1)
☐ (k)(2)
☐ (k)(3)
☐ (k)(4)
☐ (k)(5)
☐ (k)(6)
☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

2 Pages were not considered for release as they are duplicative of Doc #3, OGC/TECH. LAW UNIT FILE (pgs. 160-161)

_____ Page(s) withheld for the following reason(s): _____

☒ The following number is to be used for reference regarding these pages:
DOCUMENT #5 (Pages 463-464)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552

☐ (b)(1)
☐ (b)(2)
☐ (b)(3)
_____
_____
_____
☐ (b)(4)
☐ (b)(5)
☐ (b)(6)
☐ (b)(7)(A)
☐ (b)(7)(B)
☐ (b)(7)(C)
☐ (b)(7)(D)
☐ (b)(7)(E)
☐ (b)(7)(F)
☐ (b)(8)
☐ (b)(9)

Section 552a

☐ (d)(5)
☐ (j)(2)
☐ (k)(1)
☐ (k)(2)
☐ (k)(3)
☐ (k)(4)
☐ (k)(5)
☐ (k)(6)
☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

2 Pages were not considered for release as they are duplicative of Doc. #2, OGC/TECH. LAW UNIT FILE (PAGES 158-159)

_____ Page(s) withheld for the following reason(s): _____

☒ The following number is to be used for reference regarding these pages:
DOCUMENT #C (Pages 465-466)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

Tuesday July 18 07:02 PM EDT

Lawmakers: Stop Snooping on E-mail

WASHINGTON (APBnews.com) -- The pressure is mounting on the Justice Department to suspend a controversial new FBI wiretap system that allows agents access to vast amounts of e-mail traffic.

The so-called Carnivore system, which has come under fire from lawmakers as well as civil liberties groups since revelations about its existence surfaced last week, gives the FBI widespread access to monitor Internet service providers.

Members of Congress, led by House Majority leader Dick Armey, R-Texas, are drafting a letter they expect to send to Attorney General Janet Reno later this week urging her to put the wiretap system on hold until privacy concerns are resolved.

"The Carnivore system should not be used until concerns are addressed," Armey spokesman Richard Diamond told APBnews.com today. "There has been such a dramatic shift in what the FBI can monitor; there needs to be a public discussion. That's why the outrage. This was going on for a year and nobody knew."

Reno ordered review

Responding to concerns raised last week, Reno ordered a review of Carnivore but has no plans to order the program suspended, officials said today.

"The attorney general is looking into it to make sure she understands it and that it is applied fairly," said spokeswoman Chris Watney.

Last week Armey asked Reno and FBI Director Louis Freeh to "stop using this cybersnooping system until Fourth Amendment concerns are adequately addressed."

'The keys to the kingdom'

Rep. Bob Barr -- who described the Carnivore system surveillance abilities as "frightening" -- may demand similar restraints at a congressional oversight hearing on the program next Monday, a spokesman said.

"He is concerned about the lack of controls," said Brad Alexander, a spokesman for the Georgia Republican.

Civil libertarians, also outraged at the extent of the FBI's ability to monitor the e-mails of

Doc. #7

innocent people, also want Carnivore suspended.

"They want the keys to the kingdom," said American Civil Liberties Union Associate Director Barry Steinhardt, who is scheduled to testify at the subcommittee hearing Monday. "They want the entire stream of communications, and they expect us to trust them. Well, I don't. They have a history of abuse and stretching beyond the limits of what they are entitled to."

A critical tool, FBI says

FBI officials said they want the opportunity to demonstrate how critical the system is to its crime-fighting efforts.

"People need to know how critical this is," said bureau spokesman Paul Bresson, who said the agency wants to show the public how Carnivore works on Monday. "It gives us the ability to intercept conversations of criminals who are using the cyberworld the same way the rest of us are."

The FBI, in a statement describing Carnivore, said the system gives agents the "surgical" ability to intercept and collect information under legal orders.

Federal wiretaps have led to the convictions of 25,600 felons in the last 13 years, according to the FBI.

New wiretap rules sought

The renewed outcry comes a day after White House Chief of Staff John Podesta announced proposals that would require a more stringent approval process for FBI wiretaps, while at the same time expanding the agency's ability to conduct electronic surveillance.

The ACLU said the White House did not go far enough in its response to increasing government surveillance powers.

Steinhardt called the proposal a "camouflage for Carnivore," he said, when the administration should have "disavowed or suspended" the program. He also said the proposals stand little chance of being enacted before the Clinton administration leaves office.

The ACLU on Friday filed a Freedom of Information Act request for the source code, or computer program instructions, and other technical details about the Internet wiretapping program. The FBI said it will comply with FOIA rules and release whatever information it is able to

disclose by early August.

By Amy Worden, an APBnews.com staff writer.

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

2 Pages were not considered for release as they are duplicative of Doc. #8, OGC FRONT OFFICE FILE (PAGES 8-9)

_____ Page(s) withheld for the following reason(s): _____

X The following number is to be used for reference regarding these pages:
DOCUMENT #8 (Pages 470-471)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DO

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

1 Pages were not considered for release as they are duplicative of Doc. #4, OGC Front Office File (Page 4)

_____ Page(s) withheld for the following reason(s): _____

☒ The following number is to be used for reference regarding these pages:
DOCUMENT #9 (Page 472)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

6 Pages were not considered for release as they are duplicative of Doc. #9, OGC FRONT OFFICE FILE (PAGES 10-15)

_____ Page(s) withheld for the following reason(s): _____

☒ The following number is to be used for reference regarding these pages:
DOCUMENT #10 (Pages 473 - 478)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

9 Pages were not considered for release as they are duplicative of Doc. #18, OGC/INVESTIGATIVE LAW UNIT FILE (PAGES 445 - 453)

_____ Page(s) withheld for the following reason(s): _____

X The following number is to be used for reference regarding these pages:
DOCUMENT #11 (Pages 479 - 487)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

2 Pages were not considered for release as they are duplicative of DOC. #10, OGC FRONT OFFICE FILE (PAGES 16+17)

_____ Page(s) withheld for the following reason(s): _____

X The following number is to be used for reference regarding these pages:
DOCUMENT #12 (Pages 488-489)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

14 Pages were not considered for release as they are duplicative of DOC. # 13, PGS. 1-14, OGC FRONT OFFICE FILE (PGS. 20-33)

_____ Page(s) withheld for the following reason(s): _____

☒ The following number is to be used for reference regarding these pages:
DOCUMENT #13 (pages 490-503)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

BOB BARR
7TH DISTRICT
GEORGIA
ASSISTANT MAJORITY WHIP
PHONE (202) 225-2931
FAX (202) 225-2944
INTERNET: http://www.house.gov/barr

CONGRESS OF THE UNITED STATES
1207 LONGWORTH HOUSE BUILDING
WASHINGTON, D.C. 20515-1007

COMMITTEES
JUDICIARY
BANKING AND FINANCIAL SERVICES
GOVERNMENT REFORM
Subcommittee on Criminal Justice, Drug Policy, and Human Resources
VICE CHAIRMAN

July 24, 2000

The Honorable Louis J. Freeh
Director
Federal Bureau of Investigation
935 Pennsylvania Avenue NW
Washington, D.C. 20535-0001

IN RE: Request for Information Pertaining to Carnivore System.

Dear Director Freeh:

In light of the recent disclosure of the Bureau's use of Carnivore, and given the substantial public interest in this matter, I hereby ask to review all records concerning the Carnivore system.

Included in the records should be :

- A description of Carnivore's capability
- A history of Carnivore's development and use
- The number of cases in which Carnivore has been used, and the number of Internet Service Providers (ISP) that have had the system installed.
- An analyses of the legal issues the Bureau considered before deploying the system.

While I would welcome any explanatory information the Bureau is willing to provide in response to my inquiry, I am requesting the original, source documents themselves, and would like to receive them before August 7, 2000. Given the potential impact on the public of Carnivore, I would like to make the material I receive public, and would like the Bureau to authorize this public release.

Thank you for your cooperation. If you have any questions, please contact my Legislative Counsel, Keri Allin, at 202/225-2931. I look forward to reviewing the information.

DISTRICT OFFICES

CARROLLTON
207 NEWNAN STREET
SUITE A
CARROLLTON, GA 30117
(770) 836-1776
FAX (770) 838-0436

LAGRANGE
200 RIDLEY AVE
LAGRANGE, GA 30240
(706) 812-1776
FAX (706) 885-9019

MARIETTA
998 WHITLOCK AVE
SUITE 13
MARIETTA, GA 30064
(770) 429-1776
FAX (770) 795-9551

ROME
600 EAST 1ST STREET
ROME GA 30161
(706) 290-1776
FAX (706) 232 786-

DOC #14

With kind regards, I remain,

very truly yours,

BOB BARR
Member of Congress

BB:ka

cc: The Honorable Janet Reno
The Honorable Dennis Hastert
The Honorable Richard Armey
The Honorable Tom DeLay
The Honorable J.C. Watts
The Honorable Dan Burton
The Honorable Henry Hyde
The Honorable Charles Canady
The Honorable Bill McCollum

NEW YORK TIMES

DATE 7-23-00

PAGE WK. IN REVIEW

Learning to Live With Big Brother

By STEPHEN LABATON

WASHINGTON

IN 1928, the Supreme Court took up the case of Roy (Big Boy) Olmstead, a bootlegger whose phones had been tapped by federal agents without a warrant. The court ruled that evidence obtained in that way was legal, prompting a remarkable dissent by Judge Louis D. Brandeis.

"The progress of science in furnishing the government with the means of espionage is not likely to stop with wiretapping," Justice Brandeis wrote in a dissent that the court adopted as the law nearly 40 years later. "Ways may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home."

Thanks to the ubiquity of e-mail and the ingenuity of the F.B.I., that day has arrived. Over the last couple of weeks it has been widely reported that the F.B.I. is now using a computer program called Carnivore, which, once installed on the network of an Internet service provider, can troll through millions of e-mail messages and hone in on the electronic correspondence of suspects.

So far, the F.B.I. has reported using the program fewer than 25 times since it was developed 18 months ago, but that number is expected to grow quickly, since the bureau expects it to become an indispensable law enforcement tool, particularly in international espionage and terrorism cases.

That's fine, say critics, but Carnivore is also capable of simultaneously monitoring the communications of people not suspected of a crime. That has caused civil liberties groups and privacy advocates to worry that the technology might be used to monitor unpopular groups or political enemies, and not just suspected criminals.

Last week, as lawmakers on Capitol Hill began voicing their concerns, the White House moved to calm the growing storm. John Podesta, the president's chief of staff, outlined legislative proposals that would set legal requirements for surveillance in cyberspace.

Everyone agrees that some kind of legislation is needed to make sense of the existing patchwork of laws and court cases on electronic surveillance. At present, for example, e-mail sent via cable modem is more strictly protected than any other communication form — even telephone conversations. While law enforcement requests for lists of telephone calls to or from a particular line must be granted without question by a federal court, [illegible]

The White House proposed replacing these illogical distinctions with a uniform, rational set of standards. Civil liberties and privacy groups support this idea in principle, but are highly critical of the administration for refusing to explain how broadly it intends to use Carnivore or to describe what safeguards are in place for preventing its abuse.

"Law enforcement officials say that computer systems like Carnivore are necessary because e-mail is becoming more frequently used for communication among criminals. And the officials note that these cybermonitors can actually be set to record communications much more selectively than a phone tap.

Carnivore could, for instance, be programmed to pick up the e-mail from only one sender and a particular computer, while excluding such e-mail as messages to or from, say, the sender's lawyer or wife. Phone taps, on the other hand, pick up everything.

At a news briefing on Friday, top F.B.I. officials also announced plans to submit Carnivore to analysis by independent academics, and noted that the system kept a log of what it was asked to pick up, which could be used by a court to spot any violations.

In making their case, supporters of cybersurveillance say that the only way to track e-mail is by combing through all of the messages on a particular network, because e-mail consists of a series of digital packets that are broken apart at the sending end and transmitted along multiple electronic paths before being reconstituted by the recipient's computer.

Nonetheless, privacy groups and some Internet service providers, or I.S.P.'s, say there remains a less intrusive alternative. The providers, like AOL or the Microsoft Network, could be ordered by a court to turn over specific material, rather than give the F.B.I. unlimited access to a network. That is precisely how telephone companies are treated; they cooperate with warrants for wiretaps and lists of telephone numbers called from a particular phone.

"The real question is who should be in control," said James X. Dempsey, staff attorney for the Center for Democracy and Technology, a civil liberties group in Washington. "It upsets the balance among competing interests and privacy for law enforcement to, in essence, kick the companies out of the way, hook up a black box, and say, don't touch it."

Other experts said that it was time for a reappraisal of all the standards used by the government to eavesdrop, particularly as the world moves into an era of digital communications that can be more readily monitored by computers and more easily masked by encryption.

As even household appliances begin to be wired into the Internet and many of our most personal thoughts and associations are now shared with the computer, the issue has taken on a new imperative and is being debated on a global scale.

THE British government (whose house-to-house searches in the English colonies led to the Fourth Amendment prohibition against unreasonable searches) is near to adopting a law, the Regulation of Investigatory Powers Bill, or R.I.P., that would require Internet service companies to finance the permanent installation of a Carnivore-like system for government use.

A similar system is already in place in Russia, while in the Netherlands a debate is raging over whether the government should have the authority to tap into e-mail at all.

"This debate really cries out for a return to first principles," said Marc Rotenberg, director of the Electronic Privacy Information Center, a research organization that studies privacy issues and technology.

Among the most important of such principles, he said, is that the government should always use the least intrusive investigative techniques before taking the invasive step of trying to intercept telephone calls or e-mail messages.

"What is the solution?" he asked. "A lot of oversight, a lot of accountability, and a great deal of concern about the potential surveillance capabilities of the electronic police state."

DOC #15

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552

☐ (b)(1)
☐ (b)(2)
☐ (b)(3)
_____
_____
_____
☐ (b)(4)
☐ (b)(5)
☐ (b)(6)
☐ (b)(7)(A)
☐ (b)(7)(B)
☐ (b)(7)(C)
☐ (b)(7)(D)
☐ (b)(7)(E)
☐ (b)(7)(F)
☐ (b)(8)
☐ (b)(9)

Section 552a

☐ (d)(5)
☐ (j)(2)
☐ (k)(1)
☐ (k)(2)
☐ (k)(3)
☐ (k)(4)
☐ (k)(5)
☐ (k)(6)
☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

2 Pages were not considered for release as they are duplicative of DOC. #18, OGC FRONT OFFICE FILE (PGS. 124-125)

_____ Page(s) withheld for the following reason(s): _____

X The following number is to be used for reference regarding these pages:
DOCUMENT #16 (Pages 507-508)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DO

THE BALTIMORE SUN

July 24, 2000, Monday ,FINAL

SECTION: TELEGRAPH ,1A

LENGTH: 1119 words

HEADLINE: FBI taps of e-mail provoke concerns
Privacy issues lead to House hearings on 'Carnivore' work
Name called 'unfortunate'

BYLINE: Del Quentin Wilber

SOURCE: SUN NATIONAL STAFF

BODY:

WASHINGTON -- To civil libertarians and Internet service providers, a device created by the FBI to snoop through e-mail messages is as ominous as its name: "Carnivore."

Attached to an ISP's server, the contraption sifts through countless e-mail messages and copies specific information for federal agents seeking suspected criminals, including terrorists and child pornographers.

But critics say that, in the process of sifting out communications from its targets, Carnivore is also capable of retrieving the private messages of innocent people.

"This is a very dangerous device," said Barry Steinhardt, associate director of the American Civil Liberties Union. "It's unprecedented. It's the first time law enforcement has carte blanche access to the entire service provider's network."

The controversy surrounding the device with the foreboding name has caught the attention of Republican lawmakers, and a House Judiciary subcommittee is scheduled to hold a hearing on the matter today. Opponents and authorities who support the use of Carnivore are scheduled to testify.

After the system was disclosed in recent news accounts, sparking criticism from privacy advocates, FBI officials met with lawmakers and reporters to try to show that Carnivore is not nearly as intrusive as some fear.

For one thing, FBI officials said, they need the device to combat crime and threats to national security. They describe Carnivore as a "surgical" tool that would protect ordinary people from unintended searches.

"There are filtering mechanisms built in that limit the amount of information viewable to the human eye," said Paul Bresson, a spokesman for the bureau. "It ensures that only the exact communications authorized by a court are what we intercept."

For decades, federal agents and local police have been wiretapping suspects' phones after obtaining permission from judges. But those wiretaps are limited to a specific suspect and do not comb through phone calls at random.

Carnivore works much differently, though authorities still must obtain permission from a judge to scour e-mail messages or discover which Web pages a suspect visits.

Once they have court approval, agents attach the Carnivore device -- an ordinary- looking desktop computer -- to the ISP's main computer, and Carnivore " passively" sniffs through streams of data, FBI officials said.

Carnivore does not read e-mail messages or their subject lines, officials said. Instead, it searches for computer codes that direct the message to and from the suspect. Nor can it scan e-mail messages for key words, like "drugs or bomb," an FBI official said.

In other words, authorities say, Carnivore acts like an FBI agent authorized to scan envelopes sent by mail. The agent seeks a particular suspect's addressing information and pulls aside any qualified envelope and opens it.

Last week, after an outcry from critics, the White House said it would propose legislation to, among other things, require agents to seek Justice Department clearance before asking judges to authorize the use of Carnivore in a specific case. Such rules already cover voice wiretaps.

But the proposal was dismissed by civil liberties groups, who said it did not go far enough in protecting electronic communication.

For their part, FBI officials say, the White House proposal is not necessary: They say they abide by the rules governing voice wiretaps to use Carnivore.

Despite the assurances of FBI officials, civil liberties groups and congressional Republicans say they are wary of the system.

"It has the capability of grabbing it all," said Richard Diamond, a spokesman for Rep. Dick Armey, the Texas Republican who is the House majority leader and a sharp critic of Carnivore. "It all depends on who pushes the button. Someone could push the wrong button and have access to all sorts of information."

FBI officials dispute that assertion, though they concede that Carnivore has sometimes captured e-mail messages and data that were not targeted in their searches. They say they sealed such information and did not read it.

Earlier this year, an ISP tried unsuccessfully to prevent FBI agents from installing Carnivore on its network. After a brief court fight, the company, Earthlink, yielded to FBI demands and helped install the device.

FBI officials say they don't mind simply asking ISPs to provide them with e-mail sent by criminal suspects if that is possible. But, in most cases, agents would rather use Carnivore because it helps maintain security for criminal evidence. And many smaller ISPs are not capable of creating programs to obtain the necessary data, FBI officials said.

Though most ISPs have complied with court orders to install Carnivore, one major provider said it would refuse.

"We're not going to stand for this," said William L. Schrader, chairman and chief executive officer of PSINet Inc. "It's insidious. If they were to ask us with a court order to violate the privacy of all our customers, we would take this to the Supreme Court."

Authorities say that more criminals, especially those involved in child pornography and fraud, are increasingly using the Internet and e-mail to commit crimes.

About three years ago, agents and federal prosecutors began asking for real-time access to e-mail and Web-site visits, FBI officials said. The agents said they were worried about not having reliable and up-to-date intelligence.

FBI technicians began developing Carnivore, which was used for the first time about 18 months ago, authorities said. FBI officials declined to disclose any information about Carnivore-related cases but said the system has been used fewer than 25 times.

FBI officials said the "unfortunate" choice of a name emerged during internal discussions of the program.

At first, technicians called it "Omnivore" because it ate everything in sight. But as the system became more refined, technicians felt it needed a better name and changed it to **Carnivore:** a meat-eater.

"We're looking at how we name a lot of projects right now," an FBI official said. "This has been sobering."

FBI agents noted that they don't need **Carnivore** to read most old e-mail messages stored on ISP servers; they can already do so with court approval.

They described the **Carnivore** system as a last-resort measure to capture real-time communications.

Authorities on technology and society say they are hardly surprised that the system has generated anxiety, because many people now send more personal information over e-mail than over the phone.

Corporate snooping of employee e-mail and the unauthorized sale of client information by e-retailers have unnerved many computer users.

LOAD-DATE: July 25, 2000

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552

☐ (b)(1)
☐ (b)(2)
☐ (b)(3)
_____
_____
_____
☐ (b)(4)
☐ (b)(5)
☐ (b)(6)
☐ (b)(7)(A)
☐ (b)(7)(B)
☐ (b)(7)(C)
☐ (b)(7)(D)
☐ (b)(7)(E)
☐ (b)(7)(F)
☐ (b)(8)
☐ (b)(9)

Section 552a

☐ (d)(5)
☐ (j)(2)
☐ (k)(1)
☐ (k)(2)
☐ (k)(3)
☐ (k)(4)
☐ (k)(5)
☐ (k)(6)
☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

/ Pages were not considered for release as they are duplicative of Doc. #15, OGC FRONT OFFICE FILE (PAGE 121)

_____ Page(s) withheld for the following reason(s): _____

X The following number is to be used for reference regarding these pages:
DOCUMENT #18 (Page 512)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552

☐ (b)(1)
☐ (b)(2)
☐ (b)(3)
_____
_____
_____
☐ (b)(4)
☐ (b)(5)
☐ (b)(6)
☐ (b)(7)(A)
☐ (b)(7)(B)
☐ (b)(7)(C)
☐ (b)(7)(D)
☐ (b)(7)(E)
☐ (b)(7)(F)
☐ (b)(8)
☐ (b)(9)

Section 552a

☐ (d)(5)
☐ (j)(2)
☐ (k)(1)
☐ (k)(2)
☐ (k)(3)
☐ (k)(4)
☐ (k)(5)
☐ (k)(6)
☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

/ Pages were not considered for release as they are duplicative of Doc. #16, OGC Front Office File (Page 122)

_____ Page(s) withheld for the following reason(s): _____

X The following number is to be used for reference regarding these pages:
DOCUMENT #19 (Page 513)

XXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DO

Congressional Statement
Federal Bureau of Investigation

July 24, 2000

Statement for the Record of
Donald M. Kerr, Assistant Director
Laboratory Division
Federal Bureau of Investigation

on
Internet and Data Interception Capabilities Developed by FBI

Before the
United States House of Representatives
The Committee on the Judiciary
Subcommittee on the Constitution
Washington, D.C.

Carnivore Diagnostic Tool

Good afternoon, Mr. Chairman, and Members of the Subcommittee. I am grateful for this opportunity to discuss the Internet and data interception capabilities developed by the Federal Bureau of Investigation. The use of computers and the Internet is growing rapidly, paralleled by exploitation of computers, networks, and data bases to commit crimes and to harm the safety, security, and privacy of others. Criminals use computers to send child pornography to each other using anonymous, encrypted communications; hackers break into financial service companies systems and steal customer home addresses and credit card information; criminals use the Internet's inexpensive and easy communications to commit large scale fraud on victims all over the world; and terrorist bombers plan their strikes using the Internet. Investigating and deterring such wrongdoing requires tools and techniques designed to work with new evolving computers and network technologies. The systems employed must strike a reasonable balance between competing interests- the privacy interests of telecommunications users, the business interest of service providers, and the duty of government investigators to protect public safety. I would like to discuss how the FBI is meeting this challenge in the area of electronic mail interception.

Two weeks ago, the Wall Street Journal published an article entitled "FBI's system to covertly search E-mail raises privacy, legal issues." This story was immediately followed by a number of similar reports in the press and other media depicting our Carnivore system as something ominous and raising concerns about the possibility of its potential to snoop, without a court order, into the private E-mails of American citizens. I think that it is important that this topic be discussed openly--and in fact this was the reason we choose to share information about this capability with industry experts several weeks ago. It is critically important as technology, and particularly communications technology, a continues to evolve rapidly, that the public be guaranteed that their government is observing the statutory and constitutional protections which they demand. It is also very important that these discussions be placed into their proper context and that the relevant facts concerning this issue are made clear. I welcome this opportunity to stress that our intercept capabilities are used only after court approval and that they are directed at the most egregious violations of national security and public safety.

The FBI performs interceptions of criminal wire and electronic communications, including Internet communications, under authorities derived from Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (as amended), commonly

referred to as "Title III", and portions of the Electronic Communications Privacy Act of 1986 (as amended), or "ECPA". Such federal government interceptions, with the exception of a rarely used "emergency" authority or in cases involving the consent of a participant in the communication, are conducted pursuant to court orders. Under emergency provisions, the Attorney General, the Deputy or the Associate Attorney General may, if authorized, initiate electronic surveillance of wire or electronic communications without a court order, but only if an application for such order is made within 48 hours after the surveillance is initiated.

Federal surveillance laws apply the Fourth Amendment's dictates concerning reasonable searches and seizures , and include a number of additional provisions which ensure that this investigative technique is used judiciously, with deference to the privacy of intercepted subjects and with deference to the privacy of those who are not the subject of the court order.

For example, unlike search warrants for physically searching a house, under Title III, applications for interception of wire and electronic communications require the authorization of a high-level Department of Justice (DOJ) official before the local United State Attorneys offices can make an application to a federal court. Unlike typical search warrants, federal magistrates are not authorized to approve such applications and orders, instead, the applications are viewed by federal district court judges. Further, interception of communications is limited to certain specified federal felony offenses.

Applications for electronic surveillance must demonstrate probable cause and state with particularity and specificity: the offenses being committed, the telecommunications facility or place from which the subject's communications are to be intercepted, a description of the type of conversations to be intercepted, and the identities of the persons committing the offenses and anticipated to be intercepted. Thus, criminal electronic surveillance laws focus on gathering hard evidence–not intelligence.

Applications must indicate that other normal investigative techniques have been tried and failed to gather evidence of crime, or will not work, or are too dangerous, and must include information concerning any prior electronic surveillance regarding the subject or facility in question. Court orders are initially limited to 30 days, with extensions possible, and must terminate sooner if the objectives are met. Judges may, and usually do, require periodic reports to the court, typically every 7 to 10 days, advising it of the progress of the interception effort. This assures close and on-going oversight of the electronic surveillance by the United States Attorney's office handling the case and frequently by the court as well. Interceptions are required to be conducted in such a way as to "minimize the interception of communications not otherwise subject to interception" under the law, such as unrelated, irrelevant, and non-criminal communications of the subjects or others not named in the application.

To ensure the evidentiary integrity of intercepted communications they must be recorded, if possible, on magnetic tape or other devices, so as to protect the recording from editing or other alterations. Immediately upon the expiration of the interception period, these recordings must be presented to the federal district court judge and sealed under his or her directions. The presence of the seal is a prerequisite for their use or disclosure, or for the introduction of evidence derived from the tapes. Applications and orders signed by the judge are also to be sealed by the judge.

Within a reasonable period of time after the termination of the intercept order, including extension, the judge is obligated by law to ensure that the subject of the interception order, and other parties as are deemed appropriate, are furnished an inventory, that includes notice of the order the dates during which the interceptions were carried out, and whether or not the communication were intercepted. Upon motion, the judge may also direct that portion of the contents of the intercepted communication be made available to affected person for their inspection.

Under Title III, any person who was a part to an intercepted communication or was a party against whom an interception was directed may in any trial, hearing, or other proceeding move to suppress the contents of any intercepted communication or any evidence derived therefrom if there are grounds demonstrating that the communication was not lawfully intercepted, the order authorizing or approving the interception was insufficient on its face or the interception was not in conformance with the order.

The illegal, unauthorized conduct of electronic surveillance is a federal criminal offense punishable by imprisonment for up to five years, a fine, or both. In addition, any person whose communications are unlawfully intercepted, disclosed, or used, may recover in a civil action damages, including punitive damages, as well as attorney's fees and other costs against the person or entity engaged in the violation.

The technical assistance of service providers in helping a law enforcement agency execute an electronic surveillance order is always important, and in many cases it is absolutely essential. This is increasingly the case with the advent of advanced communication services and networks such as the Internet. Title III mandates service provider assistance incidental to law enforcement's execution of electronic surveillance orders by specifying that a court order authorizing the interception of communication shall upon the request of the applicant, direct that a telecommunications "service provider, landlord, custodian, or other person shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that such service provider, landlord, custodian, or person is according the person whose communications are to be intercepted. In practice, judges may sign two orders: one order authorizing the law enforcement agency to conduct the electronic surveillance, and a second, abbreviated, assistance order directed to the service provider, specifying, for example, in the case of E-mail, the E-mail account name of the subject that is the object of the order and directing the provision of necessary assistance.

Service providers and their personnel are also subject to the electronic surveillance laws, meaning that unauthorized electronic surveillance of their customers (or anyone else) is forbidden, and criminal and civil liability may be assessed for violations. Not only are unauthorized interceptions proscribed, but so also is the use or disclosure of the contents of communications that have been illegally intercepted. It is for this reason, among others, that service providers typically take great care in providing assistance to law enforcement in carrying out electronic surveillance pursuant to court order. In some instances, service providers opt to provide "full" service, essentially carrying out the interception for law enforcement and providing the final interception product, but, in many cases, service providers are inclined only to provide the level of assistance necessary to allow the law enforcement agency to conduct the interception.

In recent years, it has become increasingly common for the FBI to seek, and for judges to issue, orders for Title III interceptions which are much more detailed than older orders which were directed against "plain old telephone services." These detailed order, in order to be successfully implemented, require more sophisticated techniques to ensure that only messages for which there is court authorization to intercept are, in fact, intercepted. The increased detail in court orders responds to two facts.

First, the complexity of modern communications networks, like the Internet, and the complexity of modern users' communications demand better discrimination than older analog communications. For example, Internet users frequently use electronic messaging services, like E-mail, to communicate with other individuals in a manner reminiscent of a telephone call, only with text instead of voice. Such messages are often the targets of court ordered interception. Users also use services, like the world wide web, which looks more like print media than a phone call. Similarly, some Internet services, like streaming video, have more in common with broadcast media

like television, than with telephone calls. These types of communications are less commonly the targets of an interception order.

Second, for many Internet services, users share communications channels, addresses, etc. These factors make the interception of messages for which law enforcement has court authorization, to the exclusion of all others, very difficult. Court orders, therefore, increasingly include detailed instructions to preclude the interception of communications that lie outside the scope of the order.

In response to a critical need for tools to implement complex court orders, the FBI developed a number of capabilities including the software program called "Carnivore." Carnivore is a very specialized network analyzer or "sniffer" which runs as an application program on a normal personal computer under the Microsoft Windows operating system. It works by "sniffing" the proper portions of network packets and copying and storing only those packets which match a finely defined filter set programmed in conformity with the court order. This filter set can be extremely complex, and this provides the FBI with an ability to collect transmissions which comply with pen register court orders, trap & trace court orders, Title III interception orders, etc.

It is important to distinguish now what is meant by "sniffing." The problem of discriminating between users' messages on the Internet is a complex one. However, this is exactly what Carnivore does. It does NOT search through the contents of every message and collect those that contain certain key words like "bomb" or "drugs." It selects messages based on criteria expressly set out in the court order, for example, messages transmitted to or from a particular account or to or from a particular user. If the device is placed at some point on the network where it cannot discriminate messages as set out in the court order, it simply lets all such messages pass by unrecorded.

One might ask, "why use Carnivore at all?" In many instances, ISPs, particularly the larger ones, maintain capabilities which allow them to comply, or partially comply with lawful orders. For example, many ISPs have the capability to "clone" or intercept, when lawfully ordered to do so, E-mail to and from specified user accounts. In such cases, these abilities are satisfactory and allow full compliance with a court order. However, in most cases, ISPs do not have such capabilities or cannot employ them in a secure manner. Also, most systems devised by service providers or purchased "off the shelf" lack the ability to properly discriminate between messages in a fashion that complies with the court order. Also, many court orders go beyond E-mail, specifying other protocols to be intercepted such as instant messaging. In these cases, a cloned mailbox is not sufficient to comply with the order of the court.

Now, I think it is important that you understand how Carnivore is used in practice. First, there is the issue of scale. Carnivore is a small-scale device intended for use only when and where it is needed. In fact, each Carnivore device is maintained at the FBI Laboratory in Quantico until it is actually needed in an active case. It is then deployed to satisfy the needs of a single case or court order, and afterwards, upon expiration of the order, the device is removed and returned to Quantico.

The second issue is one of network interference. Carnivore is safe to operate on IP networks. It is connected as a passive collection device and does not have any ability to transmit anything onto the network. In fact, we go to great lengths to ensure that our system is satisfactorily isolated from the network to which it is attached. Also, Carnivore is only attached to the network after consultation with, and with the agreement of, technical personnel from the ISP.

This, in fact, raises the third issue - that of ISP cooperation. To date, Carnivore has, to my knowledge, never been installed onto an ISP's network without assistance from the ISP's technical personnel. The Internet is a highly complex and heterogeneous environment in which to conduct such operations, and I can assure you that without the technical knowledge of the ISP's personnel, it would be very difficult, and in some instances impossible, for law enforcement agencies to successfully implement, and

comply with the strict language, of an interception order. The FBI also depends upon the ISP personnel to understand the protocols and architecture of their particular networks.

Another primary consideration for using the Carnivore system is data integrity. As you know, Rule 901 of the Federal Rules of Evidence requires that authentication of evidence as a precondition for its admissibility. The use of the Carnivore system by the FBI to intercept and store communications provides for an undisturbed chain of custody by providing a witness who can testify to the retrieval of the evidence and the process by which it was recorded. Performance is another key reason for preferring this system to commercial sniffers. Unlike commercial software sniffers, Carnivore is designed to intercept and record the selected communications comprehensively, without "dropped packets."

In conclusion, I would like to say that over the last five years or more, we have witnessed a continuing steady growth in instances of computer-related crimes, including traditional crimes and terrorist activities which have been planned or carried out, in part, using the Internet. The ability of the law enforcement community to effectively investigate and prevent these crimes is, in part, dependent upon our ability to lawfully collect vital evidence of wrongdoing. As the Internet becomes more complex, so do the challenges placed on us to keep pace. We could not do so without the continued cooperation of our industry partners and innovations such as the Carnivore software. I want to stress that the FBI does not conduct interceptions, install and operate pen registers, or use trap & trace devices, without lawful authorization from a court.

I look forward to working with the Subcommittee staff to provide more information and welcome your suggestions on this important issue. I will be happy to answer any questions that you may have. Thank you.

| 2000 Congressional Statement | FBI Press Room | FBI Home Page |

Statement for the Record of
Donald M. Kerr
Assistant Director
Federal Bureau of Investigation
Before the
United States House of Representatives
The Committee on the Judiciary
Subcommittee on the Constitution
Washington, D.C.
7/24/2000

Good afternoon, Mr. Chairman, and Members of the Subcommittee. I am grateful for this opportunity to discuss the Internet and data interception capabilities developed by the Federal Bureau of Investigation. The use of computers and the Internet is growing rapidly, paralleled by exploitation of computers, networks, and data bases to commit crimes and to harm the safety, security, and privacy of others. Criminals use computers to send child pornography to each other using anonymous, encrypted communications; hackers break into financial service companies systems and steal customer home addresses and credit card information; criminals use the Internet's inexpensive and easy communications to commit large scale fraud on victims all over the world; and terrorist bombers plan their strikes using the Internet. Investigating and deterring such wrongdoing requires tools and techniques designed to work with new evolving computers and network technologies. The systems employed must strike a reasonable balance between competing interests - the privacy interests of telecommunications users, the business interest of service providers, and the duty of government investigators to protect public safety. I would like to discuss how the FBI is meeting this challenge in the area of electronic mail interception.

Doc. #21

Two weeks ago, the Wall Street Journal published an article entitled "FBI's system to covertly search E-mail raises privacy, legal issues." This story was immediately followed by a number of similar reports in the press and other media depicting our Carnivore system as something ominous and raising concerns about the possibility of its potential to snoop, without a court order, into the private E-mails of American citizens. I think that it is important that this topic be discussed openly–and in fact this was the reason we choose to share information about this capability with industry experts several weeks ago. It is critically important as technology, and particularly communications technology, a continues to evolve rapidly, that the public be guaranteed that their government is observing the statutory and constitutional protections which they demand. It is also very important that these discussions be placed into their proper context and that the relevant facts concerning this issue are made clear. I welcome this opportunity to stress that our intercept capabilities are used only after court approval and that they are directed at the most egregious violations of national security and public safety.

The FBI performs interceptions of criminal wire and electronic communications, including Internet communications, under authorities derived from Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (as amended), commonly referred to as "Title III", and portions of the Electronic Communications Privacy Act of 1986 (as amended), or "ECPA". Such federal government interceptions, with the exception of a rarely used "emergency" authority or in cases involving the consent of a participant in the communication, are conducted pursuant to court orders. Under emergency provisions, the Attorney General, the Deputy or the Associate Attorney General may, if authorized, initiate electronic surveillance of wire or electronic communications

without a court order, but only if an application for such order is made within 48 hours after the surveillance is initiated.

Federal surveillance laws apply the Fourth Amendment's dictates concerning reasonable searches and seizures, and include a number of additional provisions which ensure that this investigative technique is used judiciously, with deference to the privacy of intercepted subjects and with deference to the privacy of those who are not the subject of the court order.

For example, unlike search warrants for physically searching a house, under Title III, applications for interception of wire and electronic communications require the authorization of a high-level Department of Justice (DOJ) official before the local United State Attorneys offices can make an application to a federal court. Unlike typical search warrants, federal magistrates are not authorized to approve such applications and orders, instead, the applications are veiwed by federal district court judges. Further, interception of communications is limited to certain specified federal felony offenses.

Applications for electronic surveillance must demonstrate probable cause and state with particularity and specificity: the offenses being committed, the telecommunications facility or place from which the subject's communications are to be intercepted, a description of the type of conversations to be intercepted, and the identities of the persons committing the offenses and anticipated to be intercepted. Thus, criminal electronic surveillance laws focus on gathering hard evidence–not intelligence.

Applications must indicate that other normal investigative techniques have been tried and failed to gather evidence of crime, or will not work, or are too dangerous, and must include information concerning any prior electronic surveillance regarding the subject or facility in question. Court orders are initially limited to 30 days, with extensions possible, and must terminate sooner if the objectives are met. Judges may, and usually do, require periodic reports to the court, typically every 7 to 10 days, advising it of the progress of the interception effort. This assures close and on-going oversight of the electronic surveillance by the United States Attorney's office handling the case and frequently by the court as well. Interceptions are required to be conducted in such a way as to "minimize the interception of communications not otherwise subject to interception" under the law, such as unrelated, irrelevant, and non-criminal communications of the subjects or others not named in the application.

To ensure the evidentiary integrity of intercepted communications they must be recorded, if possible, on magnetic tape or other devices, so as to protect the recording from editing or other alterations. Immediately upon the expiration of the interception period, these recordings must be presented to the federal district court judge and sealed under his or her directions. The presence of the seal is a prerequisite for their use or disclosure, or for the introduction of evidence derived from the tapes. Applications and orders signed by the judge are also to be sealed by the judge.

Within a reasonable period of time after the termination of the intercept order, including extension, the judge is obligated by law to ensure that the subject of the interception order, and other parties as are deemed appropriate, are furnished an inventory, that includes notice of the order the dates

during which the interceptions were carried out, and whetehr or not the communication were intercepted. Upon motion, the jusge may also direct that portion of the contents of the intercepted communication be made available to affected person for their inspection.

Under Title III, any person who was a part to an intercepted communication or was a party against whom an interception was directed may in any trial, hearing, or other proceeding move to suppress the contents of any intercepted communication or any evidence derived therefrom if there are grounds demonstrating that the communication was not lawfully intercepted, the order authorizing or approving the interception was insufficient on its face or the interception was not in conformance with the order.

The illegal, unauthorized conduct of electronic surveillance is a federal criminal offense punishable by imprisonment for up to five years, a fine, or both. In addition, any person whose communications are unlawfully intercepted, disclosed, or used, may recover in a civil action damages, including punitive damages, as well as attorney's fees and other costs against the person or entity engaged in the violation.

The technical assistance of service providers in helping a law enforcement agency execute an electronic surveillance order is always important, and in many cases it is absolutely essential. This is increasingly the case with the advent of advanced communication services and networks such as the Internet. Title III mandates service provider assistance incidental to law enforcement's

execution of electronic surveillance orders by specifying that a court order authorizing the interception of communication shall upon the request of the applicant, direct that a telecommunications "service provider, landlord, custodian, or other person shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that such service provider, landlord, custodian, or person is according the person whose communications are to be intercepted. In practice, judges may sign two orders: one order authorizing the law enforcement agency to conduct the electronic surveillance, and a second, abbreviated, assistance order directed to the service provider, specifying, for example, in the case of E-mail, the E-mail account name of the subject that is the object of the order and directing the provision of necessary assistance.

Service providers and their personnel are also subject to the electronic surveillance laws, meaning that unauthorized electronic surveillance of their customers (or anyone else) is forbidden, and criminal and civil liability may be assessed for violations. Not only are unauthorized interceptions proscribed, but so also is the use or disclosure of the contents of communications that have been illegally intercepted. It is for this reason, among others, that service providers typically take great care in providing assistance to law enforcement in carrying out electronic surveillance pursuant to court order. In some instances, service providers opt to provide "full" service, essentially carrying out the interception for law enforcement and providing the final interception product, but, in many cases, service providers are inclined only to provide the level of assistance necessary to allow the law enforcement agency to conduct the interception.

In recent years, it has become increasingly common for the FBI to seek, and for judges to issue, orders for Title III interceptions which are much more detailed than older orders which were directed against "plain old telephone services." These detailed order, in order to be successfully implemented, require more sophisticated techniques to ensure that only messages for which there is court authorization to intercept are, in fact, intercepted. The increased detail in court orders responds to two facts.

First, the complexity of modern communications networks, like the Internet, and the complexity of modern users' communications demand better discrimination than older analog communications. For example, Internet users frequently use electronic messaging services, like E-mail, to communicate with other individuals in a manner reminiscent of a telephone call, only with text instead of voice. Such messages are often the targets of court ordered interception. Users also use services, like the world wide web, which looks more like print media than a phone call. Similarly, some Internet services, like streaming video, have more in common with broadcast media like television, than with telephone calls. These types of communications are less commonly the targets of an interception order.

Second, for many Internet services, users share communications channels, addresses, etc. These factors make the interception of messages for which law enforcement has court authorization, to the exclusion of all others, very difficult. Court orders, therefore, increasingly include detailed instructions to preclude the interception of communications that lie outside the scope of the order.

In response to a critical need for tools to implement complex court orders, the FBI developed a number of capabilities including the software program called "Carnivore." Carnivore is a very specialized network analyzer or "sniffer" which runs as an application program on a normal personal computer under the Microsoft Windows operating system. It works by "sniffing" the proper portions of network packets and copying and storing only those packets which match a finely defined filter set programmed in conformity with the court order. This filter set can be extremely complex, and this provides the FBI with an ability to collect transmissions which comply with pen register court orders, trap & trace court orders, Title III interception orders, etc.

It is important to distinguish now what is meant by "sniffing." The problem of discriminating between users' messages on the Internet is a complex one. However, this is exactly what Carnivore does. It does NOT search through the contents of every message and collect those that contain certain key words like "bomb" or "drugs." It selects messages based on criteria expressly set out in the court order, for example, messages transmitted to or from a particular account or to or from a particular user. If the device is placed at some point on the network where it cannot discriminate messages as set out in the court order, it simply lets all such messages pass by unrecorded.

One might ask, "why use Carnivore at all?" In many instances, ISPs, particularly the larger ones, maintain capabilities which allow them to comply, or partially comply with lawful orders. For example, many ISPs have the capability to "clone" or intercept, when lawfully ordered to do so, E-mail to and from specified user accounts. In such cases, these abilities are satisfactory and allow

full compliance with a court order. However, in most cases, ISPs do not have such capabilities or cannot employ them in a secure manner. Also, most systems devised by service providers or purchased "off the shelf" lack the ability to properly discriminate between messages in a fashion that complies with the court order. Also, many court orders go beyond E-mail, specifying other protocols to be intercepted such as instant messaging. In these cases, a cloned mailbox is not sufficient to comply with the order of the court.

Now, I think it is important that you understand how Carnivore is used in practice. First, there is the issue of scale. Carnivore is a small-scale device intended for use only when and where it is needed. In fact, each Carnivore device is maintained at the FBI Laboratory in Quantico until it is actually needed in an active case. It is then deployed to satisfy the needs of a single case or court order, and afterwards, upon expiration of the order, the device is removed and returned to Quantico.

The second issue is one of network interference. Carnivore is safe to operate on IP networks. It is connected as a passive collection device and does not have any ability to transmit anything onto the network. In fact, we go to great lengths to ensure that our system is satisfactorily isolated from the network to which it is attached. Also, Carnivore is only attached to the network after consultation with, and with the agreement of, technical personnel from the ISP.

This, in fact, raises the third issue - that of ISP cooperation. To date, Carnivore has, to my knowledge, never been installed onto an ISP's network without assistance from the ISP's technical

personnel. The Internet is a highly complex and heterogeneous environment in which to conduct such operations, and I can assure you that without the technical knowledge of the ISP's personnel, it would be very difficult, and in some instances impossible, for law enforcement agencies to successfully implement, and comply with the strict language, of an interception order. The FBI also depends upon the ISP personnel to understand the protocols and architecture of their particular networks.

Another primary consideration for using the Carnivore system is data integrity. As you know, Rule 901 of the Federal Rules of Evidence requires that authentication of evidence as a precondition for its admissibility. The use of the Carnivore system by the FBI to intercept and store communications provides for an undisturbed chain of custody by providing a witness who can testify to the retrieval of the evidence and the process by which it was recorded. Performance is another key reason for preferring this system to commercial sniffers. Unlike commercial software sniffers, Carnivore is designed to intercept and record the selected communications comprehensively, without "dropped packets."

In conclusion, I would like to say that over the last five years or more, we have witnessed a continuing steady growth in instances of computer-related crimes, including traditional crimes and terrorist activities which have been planned or carried out, in part, using the Internet. The ability of the law enforcement community to effectively investigate and prevent these crimes is, in part, dependent upon our ability to lawfully collect vital evidence of wrongdoing. As the Internet becomes more complex, so do the challenges placed on us to keep pace. We could not do so

without the continued cooperation of our industry partners and innovations such as the Carnivore software. I want to stress that the FBI does not conduct interceptions, install and operate pen registers, or use trap & trace devices, without lawful authorization from a court.

I look forward to working with the Subcommittee staff to provide more information and welcome your suggestions on this important issue. I will be happy to answer any questions that you may have. Thank you.

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552		Section 552a
☐ (b)(1)	☐ (b)(7)(A)	☐ (d)(5)
☐ (b)(2)	☐ (b)(7)(B)	☐ (j)(2)
☐ (b)(3)	☐ (b)(7)(C)	☐ (k)(1)
_____	☐ (b)(7)(D)	☐ (k)(2)
_____	☐ (b)(7)(E)	☐ (k)(3)
_____	☐ (b)(7)(F)	☐ (k)(4)
☐ (b)(4)	☐ (b)(8)	☐ (k)(5)
☐ (b)(5)	☐ (b)(9)	☐ (k)(6)
☐ (b)(6)		☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

2 Pages were not considered for release as they are duplicative of Doc. #18, OGC Front Office File (Pgs. 124 + 125)

_____ Page(s) withheld for the following reason(s): _____

X The following number is to be used for reference regarding these pages:
DOCUMENT #22 (Pages 530-531)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

WASHINGTON POST

DATE 7-24-02
PAGE A01

Today in Congress

SENATE

Meets at noon.
Committees:
Energy and Natural Resources—Noon. Conservation and Reinvestment Act. 366 Dirksen Senate Office Building.

HOUSE

Meets at 12:30 p.m.
Committees:
Judiciary—1 p.m. Constitution subc. Fourth Amendment issues raised by FBI's e-mail message-capturing software. 2141 Rayburn House Office Building.
Judiciary—4 p.m. Constitution subc. Constitutional amendment to make a person who has been a U.S. citizen for 20 years eligible for the office of president. 2141 RHOB.

— Reuters

Doc #24

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552

☐ (b)(1)
☐ (b)(2)
☐ (b)(3)
_____
_____
_____
☐ (b)(4)
☐ (b)(5)
☐ (b)(6)
☐ (b)(7)(A)
☐ (b)(7)(B)
☐ (b)(7)(C)
☐ (b)(7)(D)
☐ (b)(7)(E)
☐ (b)(7)(F)
☐ (b)(8)
☐ (b)(9)

Section 552a

☐ (d)(5)
☐ (j)(2)
☐ (k)(1)
☐ (k)(2)
☐ (k)(3)
☐ (k)(4)
☐ (k)(5)
☐ (k)(6)
☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

__1__ Pages were not considered for release as they are duplicative of Doc. #17, OGC FRONT OFFICE FILE (PAGE 123)

_____ Page(s) withheld for the following reason(s): _____

☒ The following number is to be used for reference regarding these pages:
DOCUMENT #25 (Page 534)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552

☐ (b)(1)
☐ (b)(2)
☐ (b)(3)
_____
_____
_____
☐ (b)(4)
☐ (b)(5)
☐ (b)(6)
☐ (b)(7)(A)
☐ (b)(7)(B)
☐ (b)(7)(C)
☐ (b)(7)(D)
☐ (b)(7)(E)
☐ (b)(7)(F)
☐ (b)(8)
☐ (b)(9)

Section 552a

☐ (d)(5)
☐ (j)(2)
☐ (k)(1)
☐ (k)(2)
☐ (k)(3)
☐ (k)(4)
☐ (k)(5)
☐ (k)(6)
☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

2 Pages were not considered for release as they are duplicative of DOC. #21, OGC FRONT OFFICE FILE (PGS. 128 + 129)

_____ Page(s) withheld for the following reason(s): _____

X The following number is to be used for reference regarding these pages:
DOCUMENT #26 (Pages 535-536)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DO

WASHINGTON POST

DATE 7-25-00
PAGE E1

FBI Makes Case For Net Wiretaps

'Carnivore' System Faces Fire on Hill

By John Schwartz
Washington Post Staff Writer

Federal law enforcement officials defended "Carnivore"—the FBI's controversial Internet wiretap system—through more than two acrimonious hours of grilling by Democratic and Republican lawmakers yesterday, painting a chilling picture of an Internet that would become a safe haven for crooks and terrorists without proper surveillance.

"Criminals use computers to send child pornography to each other using anonymous, encrypted communications," FBI Assistant Director Donald M. Kerr told the House Judiciary subcommittee on the Constitution. "Hackers break into financial service companies' systems and steal customers' home addresses and credit-card numbers, criminals use the Internet's inexpensive and easy communications to commit large-scale fraud on victims all over the world, and terrorist bombers plan their strikes using the Internet."

Many of the lawmakers seemed just as concerned with the actions of the law enforcement officials. "The potential for abuse here is tremendous," said Rep. Spencer Bachus (R-Ala.). "What you're saying is 'Trust us.'"

Carnivore is a modified version of a common network-maintenance program known as a "packet sniffer." Carnivore offers great specificity—the ability to quickly collect just the "to" and "from" information in e-mail messages, for example, and not online banking transactions. That gives law enforcement the equivalent of the telephone world's "pen register" and "trap and trace" data—the origin and destination of all calls related to the subject.

BY RAY LUSTIG—THE WASHINGTON POST

"Criminals use computers to send child pornography to each other," said FBI official Donald M. Kerr.

Civil liberties groups and Internet service providers say the system raises troubling questions about what constitutes a reasonable search and seizure of electronic data. In sniffing out potential criminal conduct, they note, the new technology also could scan private information about legal activities, taking in vast amounts of information from innocent people as well as the suspect.

The critics also note that past experience has shown that law enforcement has overstepped its wiretap authority numerous times in the past.

Barry Steinhardt, associate director of the American Civil Liberties Union, said in his testimony: "Carnivore is roughly equivalent to a wiretap capable of accessing the contents of the conversations of all the phone company's customers, with the 'assurance' that the FBI will record only conversations of the specified target."

Officials of Internet service providers who oppose the technology say they are wary of putting equipment designed by others on their networks. They want the FBI to publish information on the software used so that ISPs can be sure that it does what the agency says.

The law enforcement officials pledged to present the system to a neutral third party for review but said they cannot release so much information about the system that it will become a target for evasion and hacking.

They insisted the Carnivore system actually provides greater privacy than previous methods of gathering electronic information because it can fine-tune what the machine hands over to investigators.

The FBI's Kerr also argued that agents won't "risk their integrity, their jobs and their futures" by abusing the law.

The toughest questioning came from Reps. Jerrold Nadler (D-N.Y.) and Robert L. Barr Jr. (R-Ga.), two congressmen rarely on the same side of an issue. Nadler peppered the officials with a series of questions that underscored the point that Carnivore, under the laws that govern pen-register surveillance, could be used without the difficult showing of "probable cause" required in a telephone wiretap.

Barr cited the investigation of missing White House e-mail and scornfully said the Clinton administration asserts that "we don't even know how to keep track of our own e-mail" while "now we see a very sophisticated system for keeping track of other people's e-mails!"

After the hearing, House Majority Leader Richard K. Armey issued a statement saying members of both parties showed "strong concerns that the administration is infringing on Americans' basic constitutional protection against unwarranted search and seizure.

"Until these concerns are addressed," he concluded, "Carnivore should be shut down."

Doc. #27

WALL STREET JOURNAL

DATE 1-25-01
PAGE A24

Congressional Panel Debates Carnivore As FBI Moves to Mollify Privacy Worries

By Ted Bridis
Staff Reporter of The Wall Street Journal

WASHINGTON – The Federal Bureau of Investigation defended its Carnivore Internet-surveillance software to a largely skeptical congressional oversight panel, telling lawmakers that the electronic eavesdropping system is used only when approved by a judge and needed to protect citizens from criminals and terrorists.

To appease critics, the FBI yesterday announced a new tamper-proof auditing mechanism for Carnivore that it said will allow federal judges and others to review during each investigation how the system covertly monitors a suspect's e-mail. And the FBI said it plans to show Carnivore's inner workings to an organization that it will select to prove that the system works only as described by the government.

Members of the House Judiciary Subcommittee on the Constitution pressed FBI and Justice Department officials yesterday to prove that only e-mail and other Internet communications from criminals are harvested by the Carnivore software, whose blueprints are closely guarded. Rep. Melvin Watt (D., N.C.) raised the specter of "Big Brotherism." Rep. Henry Hyde (R., Ill.), chairman of the full Judiciary Committee, told them, "You can understand the skittishness of some people whose concern is privacy. And when you see some of the things that have happened here in Washington, it gives one reason to wonder and to worry."

"The potential for abuse here is tremendous, don't you agree?" added Rep. Spencer Bachus (R., Ala.).

"Congressman, I guess I don't agree with that," replied FBI General Counsel Larry Parkinson. And Donald Kerr, head of the FBI laboratory where Carnivore was developed, added that the software's use is subject to vigorous internal reviews, and its misuse would be a felony. "We don't have the right or the ability to just go fishing," he said.

Rep. John Conyers (D., Mich.) said, "If I could be assured that everybody wouldn't do the wrong thing because there is a statute making it criminal, that would reduce a lot of our efforts." But after Mr. Kerr offered assurances that Carnivore captures only the information it is programmed to seek, Rep. Conyers replied, "I don't know that we have any way of verifying the technological response that you're giving me."

A computer loaded with Carnivore can be plugged into an Internet-service provider's network, allowing the software to monitor the routing information for billions of distinct Internet communications such as e-mails and to make copies of full messages sent by or received from the suspect of an FBI criminal investigation. The FBI maintains that no record is kept of any unrelated messages sent by innocent customers of the same Internet provider. The FBI has used the system 16 times so far this year, in six criminal cases and 10 national-security investigations.

Critics complain that, since the government refuses to disclose the blueprints for how its software works, there is little assurance that the FBI snooping isn't broader. The American Civil Liberties Union's associate director, Barry Steinhardt, testified that the system is "roughly the equivalent to a wiretap capable of accessing the contents of the conversations of all of the phone company's customers with the assurance that the FBI will record only conversations of the specific target."

The panel discussed opening Carnivore's blueprints for review, which the FBI adamantly opposes. Even then, said Rep. Jerrold Nadler (D., N.Y.), civilian experts could be guaranteed only that they were looking at the current version of Carnivore, which is continually being upgraded and modified. "It could change at any time. You can't trust a police agency forever," he said.

Mr. Kerr said disclosing the program's code will allow computer hackers to find ways to defeat the system, and he wondered how often the code would have to be opened for review. "We would have a problem with full open disclosure," Mr. Kerr said. "When is enough enough?"

Doc #21

WASHINGTON TIMES

DATE: 7-25-00
PAGE: A1

Lawmakers rip FBI e-mail tracker

By William Glanz
THE WASHINGTON TIMES

Federal law enforcement agents say they have used the controversial Carnivore software program to track e-mail of suspects 25 times in the past two years.

But agents have never used the program illegally or tracked e-mail they were not authorized to track by a court order, FBI Assistant Director Donald Kerr told the House Judiciary subcommittee on the Constitution yesterday.

Despite the restraint the FBI says it has used, privacy rights advocates criticized law enforcement agents for using Carnivore and lawmakers expressed skepticism about the federal government's use of the Internet surveillance tool.

House Majority Leader Dick Armey, Texas Republican, said yesterday Carnivore should be suspended until concerns of privacy advocates and needs of law enforcement are reconciled.

"Until these concerns are addressed, Carnivore should be shut down," he said.

Carnivore enables investigators to "pick out" specific e-mail messages traveling through an Internet service provider's computer system so it can monitor who a suspect contacts and who contacts a suspect.

Mr. Kerr and other federal officials said the high-tech surveillance system is crucial to help them keep up with an increasingly sophisticated breed of tech-savvy criminals and crucial to help them keep the Internet safe.

"Many of the crimes that we confront every day in the physical world are beginning to appear on line," said Deputy Assistant Attorney General Kevin DiGregory. "[We] fail to make the Internet safe ... confidence in using the Internet and E-commerce will [be] endangering the very ... the information ... Carnivore is simply an ... that is used on ... narrowly defined ... only when au... to meet our re... public," he ...

Surveillance tool employed 25 times

But lawmakers expressed concern about a lack of checks and balances on law enforcement agents using Carnivore.

"The potential for abuse here is enormous," said Rep. Spencer Bachus, Alabama Republican.

FBI General Counsel Larry Parkinson said Carnivore is a little-used tool. When it is used, Mr. Kerr said, agents follow the law carefully, and if they are caught collecting more data than allowed, they can be imprisoned up to five years for committing a federal felony.

"In the past, we've had many agencies go beyond the scope of their authority," said Rep. John Conyers Jr., Michigan Democrat.

Mr. Kerr said the FBI and Department of Justice will seek an independent review of Carnivore this year to show they aren't misusing the program.

Lawmakers and privacy rights advocates also criticized federal officials for using Carnivore when Internet service providers could just as easily collect information being sought.

"There ought to be more control in the hands of the [Internet service providers]," said Alan Davidson, a lawyer with the District-based civil liberties group Center for Democracy and Technology.

Mr. Kerr argued that few of the nation's estimated 10,000 Internet service providers have the means to sift through e-mail traffic and collect them for law enforcement.

But Robert Corn-Revere, an attorney who represented Atlanta-based Internet service provider EarthLink, said EarthLink was gathering e-mail information at the federal government's request earlier this year when it was forced to comply with a court order and let federal officials install Carnivore on its computers.

The federal government was upset that EarthLink was capturing few e-mail messages, Mr. Corn-Revere said, and it needlessly installed Carnivore.

American Civil Liberties Union Associate Director Barry Steinhardt suggested Carnivore's source code be made public. The source code is the set of instructions a programmer writes, and it will show just what Carnivore is capable of retrieving. The ACLU has filed a Freedom of Information Act request with the FBI to get the source code.

Even though they had a raft of questions about Carnivore and its use, lawmakers yesterday didn't express any willingness to make immediate changes in the federal government's authority to use the surveillance program.

"We should be sensitive to any potential for abuse of the Carnivore system. Even a system designed with the best of intentions to legally carry out essential law enforcement functions may be a cause for concern if its use is not properly monitored," said Rep. Charles T. Canady, Florida Republican.

Doc 29

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552

☐ (b)(1)
☐ (b)(2)
☐ (b)(3)
_____
_____
_____
☐ (b)(4)
☐ (b)(5)
☐ (b)(6)
☐ (b)(7)(A)
☐ (b)(7)(B)
☐ (b)(7)(C)
☐ (b)(7)(D)
☐ (b)(7)(E)
☐ (b)(7)(F)
☐ (b)(8)
☐ (b)(9)

Section 552a

☐ (d)(5)
☐ (j)(2)
☐ (k)(1)
☐ (k)(2)
☐ (k)(3)
☐ (k)(4)
☐ (k)(5)
☐ (k)(6)
☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

__/__ Pages were not considered for release as they are duplicative of Doc #20, OGC FRONT OFFICE FILE (PG. 127)

_____ Page(s) withheld for the following reason(s): _____

X The following number is to be used for reference regarding these pages:
DOCUMENT #30 (Page 540)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

FBI/DO

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

_____ Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

☐ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552

☐ (b)(1)
☐ (b)(2)
☐ (b)(3)
_____
_____
_____
☐ (b)(4)
☐ (b)(5)
☐ (b)(6)
☐ (b)(7)(A)
☐ (b)(7)(B)
☐ (b)(7)(C)
☐ (b)(7)(D)
☐ (b)(7)(E)
☐ (b)(7)(F)
☐ (b)(8)
☐ (b)(9)

Section 552a

☐ (d)(5)
☐ (j)(2)
☐ (k)(1)
☐ (k)(2)
☐ (k)(3)
☐ (k)(4)
☐ (k)(5)
☐ (k)(6)
☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

_____ Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

_____ Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

1 Pages were not considered for release as they are duplicative of Doc #19, OGC Front Office File (pg. 126)

_____ Page(s) withheld for the following reason(s): _____

☒ The following number is to be used for reference regarding these pages:
DOCUMENT #31 (Page 541)

XXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

AMERICAN CIVIL LIBERTIES UNION

Barry Steinhardt
Associate Director

National Headquarters 125 Broad Street, New York, NY 10004-2400

Tel (212) 549-2508 Fax (212) 549-2651

July 26, 2000

John Kelso Jr.
Federal Bureau of Investigation
Chief, FOI/PA Section, Rm. 6296 JEH
Washington, D.C. 20535-0001

Office of Public Affairs
United States Department of Justice
Room 1128
950 Pennsylvania Avenue NW
Washington DC 20530-0001

Attention:

We are writing pursuant to the Freedom of Information Act (5 U.S.C. § 552) to request expedited handling of our July 14, 2000 request for all agency records (including letters, correspondence, tape recordings, notes, data, memoranda, email, computer source and object code, technical manuals, technical specifications, or any other materials) held by the Federal Bureau of Investigation (FBI) regarding the following:

1. The computer system, software or device known as "Carnivore", which has been or is currently used by the FBI in connection with trap and trace and pen register orders served on Internet Service Providers or in connection with orders for the interception of the content of electronic communications served on Internet Service Providers;

2. The computer system, software or device known as "Omnivore", which has been or is currently used by the FBI in connection with trap and trace and pen register orders served on Internet Service Providers or in connection with orders for the interception of the content of electronic communications served on Internet Service Providers, and

3. The computer system, software or device known as "EtherPeek", which has been or is currently used by the FBI in connection with trap and trace and pen register orders served on Internet Service Providers or in connection with orders for the interception of the content of electronic communications served on Internet Service Providers.

We seek expedited review of this FOIA request because this information relates to impending policy decisions to which informed members of the public might contribute.

Timely public access to these materials is necessary to fully inform the public about the issues surrounding communications interception and related technological developments.

Specifically, we request expedited access pursuant to 28 C.F.R. 16.5(d)(1)(ii), which allows such processing based on an "urgency to inform the public about an actual or alleged government activity, if made by a person primarily engaged in disseminating information." As explained earlier, the Federal government's use of Carnivore is a matter of great importance because it raises serious questions as to the government's willingness to protect individual privacy and civil liberties. Note that public interest about Carnivore has been so strong that Congress has seen fit to hold at least one hearing on this subject. (See *Oversight Hearing on "Fourth Amendment Issues Raised by the FBI's 'Carnivore' Program,"* 106th Cong. (2000).) A recent Congressional hearings and slew of press coverage indicate the "urgency to inform the public" on this issue. (See, e.g., John Schwartz, "Republicans Oppose FBI Scrutiny of E-Mail," Washington Post, July 21, 2000 at A1; D. Ian Hopper, "Eating Away at Privacy?" Associated Press, July 12, 2000; "Eyeing High-Tech Private Eyes," ABCNews.com, July 14, 2000; "FBI says Carnivore will not devour privacy," CNN.com, July 21, 2000; Margaret Johnston, "FBI Demos E-Mail 'Carnivore'," PC World.com, July 21, 2000.)

Moreover, the American Civil Liberties Foundation (ACLU Foundation) meets the criterion laid out in National Security Archive v. Department of Defense, where a representative of the news media is defined as an entity that "gathers information of potential interest to a segment of the public" and "uses its editorial skills to turn raw materials into a distinct work, and distributes that work to an audience." 881 F. 2d at 1387. The ACLU Foundation publishes newsletters, frequent press releases, news briefings, right to know handbooks, and other materials that are disseminated to the public. Its material is widely available to everyone including tax exempt organizations, not-for-profit groups, law students and faculty through its public education department. The ACLU Foundation disseminates information through publications available on-line at www.aclu.org as well. Thus the organization meets the pertinent regulatory requirements for expedited access.

In addition, we request expedited access pursuant to 28 C.F.R. 16.5(d)(1)(iv), which allows such access for a "matter of widespread and exceptional media interest in which there exist possible questions about the government's integrity which affect public confidence." Again, the recent Congressional hearings, as well as the storm of media coverage about Carnivore and related computer programs provide ample evidence of the "widespread and exceptional media interest" in this issue. Moreover, the revelations about Carnivore raise doubts as to the government's integrity in safeguarding the privacy of individuals.

We have enclosed certification (for the purposes of expedited access) with this letter.

If our request is denied in whole or part, we ask that you justify all deletions by reference to specific exemptions of the act. We expect you to release all segregable portions of otherwise exempt material. We reserve the right to appeal your decision to withhold any information or to deny a waiver of fees.

We look forward to your reply within ten calendar days, as required under 28 C.F.R. 16.5(d)(4).

Thank you for your assistance.

Sincerely,

Barry Steinhardt, Esq.
On behalf of the ACLU Foundation

Enclosures

CERTIFICATION

To whom it may concern:

I certify that the following facts are true and correct to the best of my knowledge and belief:

1. The American Civil Liberties Foundation (ACLU Foundation) meets the criterion laid out in National Security Archive v. Department of Defense, where a representative of the news media is defined as an entity that "gathers information of potential interest to a segment of the public" and "uses its editorial skills to turn raw materials into a distinct work, and distributes that work to an audience." 881 F. 2d at 1387. The ACLU Foundation publishes newsletters, frequent press releases, news briefings, right to know handbooks, and other materials that are disseminated to the public. Its material is widely available to everyone including tax exempt organizations, not-for-profit groups, law students and faculty for no cost or for a nominal fee through its public education department. The ACLU Foundation disseminates information through publications available on-line at www.aclu.org as well.

2. The disclosure of information regarding the following computer systems is in the public interest:

- The computer system, software or device known as "Carnivore", which has been or is currently used by the FBI in connection with trap and trace and pen register orders served on Internet Service Providers or in connection with orders for the interception of the content of electronic communications served on Internet Service Providers;

- The computer system, software or device known as "Omnivore", which has been or is currently used by the FBI in connection with trap and trace and pen register orders served on Internet Service Providers or in connection with orders for the interception of the content of electronic communications served on Internet Service Providers, and

- The computer system, software or device known as "EtherPeek", which has been or is currently used by the FBI in connection with trap and trace and pen register orders served on Internet Service Providers or in connection with orders for the interception of the content of electronic communications served on Internet Service Providers.

Records regarding Carnivore, Omnivore and EtherPeek are likely to contribute significantly to the public understanding of the activities of the government. The ACLU Foundation is a nonprofit 501(c)3 research and education organization working to increase citizen participation in governance issues. The ACLU Foundation is making this request specifically for the public's enhanced understanding of lawfully authorized wiretapping, its relationship to constitutional guarantees of privacy as well as an

understanding of global technological developments in wire and electronic networks that facilitate and expedite such wiretapping. The public's interest is particularly pertinent in light of advancing communications technology and the rapid growth of the World Wide Web. These developments have greatly increased the communications interconnectedness of all the countries in the world, especially technologically advanced nations like the US and the Netherlands.

3. The information requested regards a "matter of widespread and exceptional media interest in which there exist possible questions about the government's integrity which affect public confidence." Public interest in Carnivore has grown to such an extent that Congress has held at least one hearing on this subject. (See *Oversight Hearing on "Fourth Amendment Issues Raised by the FBI's 'Carnivore' Program,"* 106th Cong. (2000).) The tremendous amount of media coverage about Carnivore and related computer programs also provides strong evidence of the "widespread and exceptional media interest" in this issue. (See, e.g., John Schwartz, "Republicans Oppose FBI Scrutiny of E-Mail," Washington Post, July 21, 2000 at A1; D. Ian Hopper, "Eating Away at Privacy?" Associated Press, July 12, 2000; "Eyeing High-Tech Private Eyes," ABCNews.com, July 14, 2000; "FBI says Carnivore will not devour privacy," CNN.com, July 21, 2000; Margaret Johnston, "FBI Demos E-Mail 'Carnivore'," PC World.com, July 21, 2000.) In addition, the requested material may provide answers to serious questions regarding the government's willingness to protect individual privacy and civil liberties.

Barry Steinhardt, Esq.
On behalf of the ACLU Foundation

7/26/00

July 26, 2000

CARNIVORE Diagnostic Tool

Internet and Data Interception Capabilities Developed by the FBI, Statement for the Record, U.S. House of Representatives, the Committee on the Judiciary, Subcommittee on the Constitution, 07/24/2000, Laboratory Division Assistant Director Dr. donald M. Kerr

The Nation's communications networks are routinely used in the commission of serious criminal activities, including espionage. Organized crime groups and drug trafficking organizations rely heavily upon telecommunications to plan and execute their criminal activities.

The ability of law enforcement agencies to conduct lawful electronic surveillance of the communications of its criminal subjects represents one of the most important capabilities for acquiring evidence to prevent serious criminal behavior. Unlike evidence that can be subject to being discredited or impeached through allegations of misunderstanding or bias, electronic surveillance evidence provides jurors an opportunity to determine factual issues based upon a defendant's own words.

Under Title III, applications for interception require the authorization of a high-level Department of Justice (DOJ) official before the local United States Attorneys offices can apply for such orders. Interception orders must be filed with federal district court judges or before other courts of competent jurisdiction. Hence, unlike typical search warrants, federal magistrates are not authorized to approve such applications and orders. Further, interception of communications is limited to certain specified federal felony offenses.

Applications for electronic surveillance must demonstrate probable cause and state with particularity and specificity: the offense(s) being committed, the telecommunications facility or place from which the subject's communications are to be intercepted, a description of the types of conversations to be intercepted, and the identities of the persons committing the offenses that are anticipated to be intercepted. Thus, criminal electronic surveillance laws focus on gathering hard evidence -- not intelligence.

Applications must indicate that other normal investigative techniques will not work or are too dangerous, and must include information concerning any prior electronic surveillance regarding the subject or facility in question. Court orders are limited to 30 days and interceptions must terminate sooner if the objectives are obtained. Judges may (and usually do) require periodic reports to the court (typically every 7-10 days) advising it of the progress of the interception effort. This circumstance thus assures close and ongoing oversight of the electronic surveillance by the United States Attorney's office handling the case. Extensions of the order (consistent with requirements of the initial application) are permitted, if justified, for up to a period of 30 days.

Electronic surveillance has been extremely effective in securing the conviction of more than 25,600 dangerous felons over the past 13 years. In many cases there is no substitute for electronic surveillance, as the evidence cannot be obtained through other traditional investigative techniques.

In recent years, the FBI has encountered an increasing number of criminal investigations in which the criminal subjects use the Internet to communicate with each other or to communicate with their victims. Because many Internet Service Providers (ISP) lacked the ability to discriminate communications to identify a particular subject's messages to the exclusion of all others, the FBI designed and developed a diagnostic tool, called Carnivore.

The Carnivore device provides the FBI with a "surgical" ability to intercept and collect the

Stop Carnivore
July 27, 2000

Twenty-eight Members of Congress sent the following letter to Attorney General Janet Reno asking her to suspend operation of the Carnivore Internet surveillance system until the serious privacy issues involved have been addressed.

Congress of the United States

Washington, DC 20515

July 27, 2000

The Honorable Janet Reno, Attorney General
US Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530-0001

Dear Attorney General Reno,

We are writing to express our strong reservations about a new Internet monitoring system developed by the Federal Bureau of Investigation, called Carnivore.

Carnivore, it has been reported, enables the Federal Government to scan all of the traffic on an Internet Service Provider's network. Although national security and law enforcement are essential priorities, Carnivore has raised serious Fourth Amendment questions. Should the federal government be trusted with this kind of personal communication?

Consumer confidence in the privacy and security of the Internet are essential for continued growth of e-commerce. People should feel secure that the federal government is not reading their email, no matter how worthy the objective.

Given the uproar Carnivore has created, and the potential impact reports on Carnivore could have on consumer confidence in the Internet, we urge you to suspend any activity involving the development or use of Carnivore until the serious privacy issues involved have been satisfactorily answered.

Sincerely,

Dick Armey	Tom DeLay	J.C. Watts
Kevin Brady	John Thune	Larry Combest
Jack Metcalf	Brian Bilbray	Julia Carson
Charlie Norwood	Bob Barr	Bill Archer
Nancy Johnson	Jim McCrery	Terry Everett
Richard Pombo	John McHugh	Tom Campbell
Sonny Callahan	Jim Kolbe	Donald A. Manzullo
Tom Coburn	Richard Baker	Zach Wamp
Charles H. Taylor	Mac Thornberry	Jim Gibbons
Dan Miller		

Additional supporters:

Cynthia McKinney	Doc Hastings	Bob Goodlatte
Ron Paul		

Related Links

The e-Contract

Remarks on the e-Contract with High Tech America

WebVote: Internet Privacy

Stop Carnivore

More Questions About FBI Cybersnooping System

WebVote